The Global State of Scams - 2021

How are countries worldwide fighting online scams?

€ 41.3 Billion lost in Scams, up 15%

Law enforcement worldwide received 266 million reports from scam victims

With the Corona pandemic, the scam industry boomed worldwide. In our 3rd Global State of Scam Report, we analyzed 42 countries focusing on the number of people scammed, the amount of money lost and the ways in which national governments, consumer authorities and law enforcement are combating scams.

Number of Scams Boomed

The number of reported scams increased from 139 in 2019 to 266 million in 2020. The massive growth is caused mainly due to the COVID-pandemic, and in part as more countries have started to report online fraud.

While the definitions and reporting methods used by different countries for scams differ strongly, nearly all nations have reported large increases in the number of reported scams. Egypt (190%) and Nigeria (186%) reported the most dramatic increase in the number of scams. Other developing countries such as Iran, India and Pakistan also reported a strong growth in the number of scams of around 90% as the population massively moved to the internet. Only a few countries reported minor decreases including Belgium, Japan and Sweden.

The amount lost grew from € 36 ($ 41.7) to € 41 billion ($ 47.8). The number of scams and money lost is likely to be only a small fraction of the actual size of online fraud. Depending on the country, less than 3% and up to 15% of consumers report a scam. Based on a previous study by ScamAdviser, the cause behind these numbers lies in that 23% of consumers do not know where to report scams and 11% do not think it will make any difference.

Investment scams are on the rise

The money lost per victim and the type of scams differ strongly by country. From less than €10 for counterfeiters and subscription traps to hundreds of thousands for ransomware, Business Email Compromise (BEC) and investment scams.

While phishing continues to be the most common type of scam globally, the pandemic has introduced new twists on old scams. In 2020, scammers first focused on masks, respirators, and disinfectants. Moving forward, they introduced 'COVID-19 charities', 'vaccine pre-registration' and 'get your Corona government grant'.

New scams popped up as well. As families were looking for a pet during the lockdown, pet scams, where a puppy ordered never arrived, gained traction. Scammers also became better at 'up-selling'. Delivery scams in which the victim first buys a product that never ships, and then is charged "custom fees" by the same scammer, boomed. Scammers are able to translate news into scams within hours. For instance, they used bush fires in Australia for charity hoaxes and the Evergreen containership crisis for investment scams.

Some scams seem to be region-specific. Australia reported an increase of 140% in threat-based scams, which typically involve scammers threatening victims with arrest, deportation or legal action unless money is paid. Likewise, Malaysia reported an increase of 450% in "Macau" scams where a fake bank, government or police officer approaches the victim with a fee that must be paid within hours or consequences have to be faced. Switzerland has proven to be extremely vulnerable to investment scams, reporting the highest amount stolen per report of more than € 25,000.

There is also a clear trend of personalizing scams based on data gathered from hacks and the use of local languages. Finland, for example, reported a 15% increase in online fraud where phishing scams are increasingly translated to Finnish.

COVID-19 also introduced seemingly unrelated increases of "drivers licence scams" and "thesis writing extortions". Huge queues for taking a driver's license exam in Germany and Ireland made people more prone to order a fake license online. The same applies to students worldwide searching for support when writing a an academic paper or thesis. In both cases the document never arrives, and the victim is unlikely to report the scam to the authorities.

With the "zero-interest" economy and boredom, many - especially males - proved to be willing victims to "investment opportunities". These scams, also called 'pig-butchering', can run for 3, 6 or even 12 months. The scammer builds up a trusted and sometimes romantic relationship with the victim before inviting him to invest in an 'incredible opportunity'.

Countries are becoming creative

To fight scams, many countries have resorted to more aggressive annual awareness campaigns. However, results seem to be mixed. As the themes of the scam change (e.g. pet scams, COVID grants), citizens worldwide still seem to fall for them, despite earlier warnings.

A strategy applied by the Irish police seems a cheaper and more effective strategy. Each week a new kind of scam is published on social media and pushed to both local and national media agencies. This strategy helps to keep cybercrime in the minds of consumers who could fall victim to various scams.

Simple changes can sometimes have big impacts. The government of Iran, for example, made two-factor authentication mandatory for banking apps. As a result, the number of banking phishing scams dropped by 90% in one year.

The Center for Cybersecurity Belgium (CCB) launched an email address to report phishing emails. It has proven to be a huge success. In 2020, the CCB received 3.2 million emails. The data collected is used to feed Internet filters, protecting Belgium citizens from malicious domains.

Likewise, the government of Taiwan has launched an Open Data Initiative, sharing cybercrime related data with both government organizations, non-profits and commercial organizations to combat online fraud.

Some countries are trying new approaches. For instance, Pakistan is training CyberScouts, who can be police officers as well as students and youngsters. Goal: ingrain cybercrime awareness in local communities.

The Japanese Minami Precinct launched Operation "Pretend to Be Fooled". This new crime-fighting program asks people who have been contacted by someone claiming to be a family member or friend in need of cash to notify the police. The potential victim and the police then work together to catch the scammer. The target victim receives a reward of 10,000 yen (€ 77.-).

Too Little; Too Late?

In recent years, the attention of governments has mainly been on "larger cybercrimes", hacks, DDOS attacks, BEC and ransomware. However, this is rapidly changing, in some cases because a (prime) minister publicly fell for a phishing scam, as occurred in Pakistan and South Africa.

In terms of the money lost, scams now make up 5% of total cybercrime, estimated by McAfee to be € 815 billion ($ 945) billion in 2020. In terms of volume, online scams are a much bigger part of cybercrime. According to Group-IB, scam and phishing account for 73% of all cyberattacks.

Due to the strong increase in scams, online security firms are scaling up. Trend Micro, for example, is heavily investing in new anti-scam services, such as the real-time scam detection tool Trend Micro Check. In 2021 they already blocked more than 2.4 billion phishing emails and scam site visits.

Due to the strong increase in scams, online security firms are scaling up. Trend Micro, for example, is heavily investing in new anti-scam services, such as Trend Micro Check. In 2021 they already blocked more than 2.4 billion phishing emails and scam site visits.

Countries' policies for fighting scams differ strongly. English-speaking countries seem to take the lead with intensive awareness campaigns, centralized online reporting on sites like Fraud UK and ScamWatch Australia and centralized special cybercrime units such as the FBI IC3 and the Canadian Anti-Fraud Center.

In other countries, scam reporting is fragmented across well-willing government initiatives, public-private partnerships, and local police units with little to no cybersecurity experience. In developing countries, such as Kenya and Pakistan, victims sometimes have to travel hundreds of miles to report a scam physically at a local police station only to be turned down by a police officer stating that the victim "should have known better".

How can we Turn the Tide?

In many countries, scams are now the most reported form of crime. In Sweden, fraud made up 5% of all crime cases reported in 2000. Now, this value is 17%. In the UK and the USA, scams are in 2021 the most commonly experienced form of crime. Finally, Singapore states that 44% of all reported crimes are related to online scams.

The World Economic Forum estimates that 0.05% of all cybercrime is prosecuted. This makes scams, which are even more underreported than "big cybercrimes", a very lucrative business.

While many developing countries are now focusing on building cybercrime awareness amongst their populations, more industrialized countries have learned that education alone is not enough.

Spain, with its 017-initiative accessible via phone, WhatsApp and Telegram and the Netherlands with easier online reporting have seen a strong growth in reported cybercrime. While this may not look good in police statistics, better data is the first step to fighting back.

The next step is increased national sharing of data. In the USA, the Federal Trade Commission is taking a leading role in gathering all scam-related data, collecting and sharing data with 3,000 federal, state, and local law enforcers across the country. Likewise, ScamWatch Australia is intensifying cooperation with Australian law enforcement, the Financial Regulation Commission, banks, telecom operators and social media companies.

In Europe and Australia, new legislation is making banks more responsible for phishing and investment scams. If the scam could have been prevented by the bank, the victims have to be compensated for their loss. This has spurred banking associations to fund anti-phishing campaigns. According to several countries, the next action to take, should be for tech giants to take more responsibility, using their own data to better identify and prevent scams.

While the USA, Canada and Australia have started sharing scam data amongst each other, most countries still linger. Yet, sharing online fraud data globally is the only real solution to turning the tide on the worldwide epidemic of scams as it allows faster identification, prevention, investigation and prosecution. A lot of work remains to be done.

As the number and amounts lost in scams continue to increase, I do hope this 3rd Global State of Scams report will help you gain insights into how other nations are fighting online cybercrime and inspire you to join forces.

Best regards,

Jorij Abraham

General Manager
ScamAdviser

A big "thank you" to our supporting members

Foundation Members

GROUP iB
GLOBAL CYBER SECURITY COMPANY

TREND MICRO™

euroDNS
YOUR WORLD OF DOMAIN NAMES

ever
Nothing to hide. Everything to gain.

EBRAND

Corporate Members

builtWith

cira

OI CYBERA

CYBERTRACE

DomainCrawler

FlashStart®
INTERNET PROTECTION

F-Secure

globaleyez

kaspersky

moosend

netsweeper

Xolphin
A SECTIGO COMPANY

WEBROOT
an opentext company

Want to join our fight against online scams? Join us!

The following people contributed to this report

Name	Organization	Country
Diego Migliorisi	Asociación Argentina de Lucha contra el Cibercrimen (AALCC)	Argentina
Miguel Angel Quevedo	Asociación Argentina de Lucha contra el Cibercrimen (AALCC)	Argentina
Alex Meaney	Scamwatch Australia (ACCC)	Australia
Jayde Richmond	Scamwatch Australia (ACCC)	Australia
Thorsten Behrens	Österreichisches Institut für angewandte Telekommunikation (OIAT)	Austria
Miguel De Bruycker	Center for Cyber Security Belgium	Belgium
Érico Rodrigues de Melo	PROCON Brazil	Brazil
Fabio Ramos	Axur	Brazil
Alexandra Tsvetkova	LIBRe Foundation	Bulgaria
Vladimir Dimitrov	Police Bulgaria	Bulgaria
Janet Naidenova	Bulgarian E-commerce Association	Bulgaria
Guy Paul Larocque	Police Canada (Canadian Anti-Fraud Centre)	Canada
Julie Wilson		Canada
Mark Gaudet	CIRA, The Canadian Internet Registration Authority	Canada
JJ Pan Chaochuan	World Trust Alliance (WTA)	China
Li-Xiong Chu	Dr2 Consultants Shanghai	China
Stefanie Ros	Dr2 Consultants Shanghai	China
Tiffany Zhang	Dr2 Consultants Shanghai	China
Mohamed Chawki	The Council of State	Egypt
Kati Bjorninen	Independent Consultant	Finland
Kristian Meismaa	Police Finland	Finland
Éric Freyssinet	Gendarmerie Nationale	France
Stephane Robinot	Europol	France
Karin Potel	Reuschlaw, Legal Consultants	Germany
Stefan Hessel	Reuschlaw, Legal Consultants	Germany
Tushar Bhagat	SAFECOM Internet and Ecomm Safety Foundation	India
Amir Hosein Tangsiri Nezhad	Gatebreakers Foundation	Iran
Behrang Taghizadeh	OIEC Group	Iran
Taha Sarhangi	IRAN Telecommunication Research Center (ITRC)	Iran
Michael Cryan	Police Ireland (An Garda Síochána)	Ireland
Federico Cavallo	Altroconsumo	Italy
Ivano Daelli	Altroconsumo	Italy
Eiichiro Mandai	ODR Room Network	Japan
Satoru Shimane	Japan Cybercrime Control Center (JC3)	Japan
Hasnida Zainuddin	Cybersecurity Malaysia	Malaysia
Saral James	Malaysian Association Of Standards Users	Malaysia
Saravanan Thambirajah	Federation of Malaysian Consumer Associations (FOMCA)	Malaysia
Pablo Corona Fraga	Associacion de Internet Mexico (AIMX)	Mexico
Philippe Boulanger	Associacion de Internet Mexico (AIMX)	Mexico
Laurens Messing	Betaalvereniging / Currence	Netherlands
Tanya Wijngaarden	Fraudehelpdesk	Netherlands
Sean Lyons	Netsafe New Zealand	New Zealand
Confidence Staveley	CyberSafe Foundation	Nigeria
Enyinna Abazie	CyberSafe Foundation	Nigeria
Terdoofan Agber	CYBER COMPOUND	Nigeria
Asif Riaz	Digital Arrays	Pakistan
Ayesha Masood	Digital Rights Foundation	Pakistan
Muhammad Asad Ul Rehman	Cyber Security of Pakistan	Pakistan
Frederic Albert De Vera	Cybercrime Investigation and Coordinating Center (CICC)	Philippines
Gil Tario	Cyber Security Philippines CERT	Philippines
Nathaniel Rabonza	Cybercrime Investigation and Coordinating Center (CICC)	Philippines
Wojciech Szczerba	European Consumer Center (ECC) Poland	Poland
Covita Sónia	Altroconsumo	Portugal
Bogdan Ciinaru	Europol	Romania
Dmitry Tunkin	Group-IB	Russia
Alisa Kayfadzhyan	Group-IB	Russia
Dmitry Lobanov	RLab Realty	Russia
Mohammed Iraqi	Consumer Protection Association, Saudi Arabia	Saudi Arabia
Elissa Chong	National Crime Prevention Council Singapore (NCPC)	Singapore
Anna Collard	Knowbe4	South Africa
Craig Pedersen	TCG Digital Forensics	South Africa
Louise van der Merwe	South African Banking Risk Information Center	South Africa
Willem Marais	Standard Bank of South Africa	South Africa
You Jung Kee	Interpol	South Korea
Alejandro Fernández-Cernuda	Global Cyber Alliance	Spain
Anton Lonnebo	Police Sweden	Sweden
Jan Olsson	Police Sweden	Sweden
Nicola Staub	Cybera.io	Switzerland
Kalin Chih	Trend Micro	Taiwan
Isıl Özden	UITSEC International	Turkey
Laçin Özer	Kilinc Law & Consulting	Turkey
Maksym Dvorovyi	Digital Security Lab Ukraine	Ukraine
Oleksii Padenko	Interpol	Ukraine
Andy Bates	Global Cyber Alliance	United Kingdom
Donna Gregory	Federal Bureau of Investigation (FBI)	United States of America
Hieu Minh Ngo	Chong Lua Dao	Vietnam
Luong Van Cua	scamvn.com	Vietnam

We sincerely thank them for their support and feedback

SCAMADVISER

How did we collect the data?

We used desk research to find country related cybercrime statistics. Unfortunately, most countries do not yet have ready made available statistics on online scams. In some cases, we had to report the number of cyber-incidents or frauds (both online as well as offline) as these were the only data available.

We also used LinkedIn to search for national experts in the area of cybercrime. In many cases we were able to contact the national (cyber)police. We asked these expert to provide and/or verify the collected data.

The key sources per country are listed on each country page. Additional sources used are available at request.

For population and GDP related data we used the World Bank. The number of Internet users was retrieved from Internet World Stats. For currency conversion XE.com mid-market exchange was applied. The source of the flags is CountryFlags.com.

Egypt and Nigeria report the highest growth in scams

SCAMADVISER

% growth in online fraud 2019 - 2020
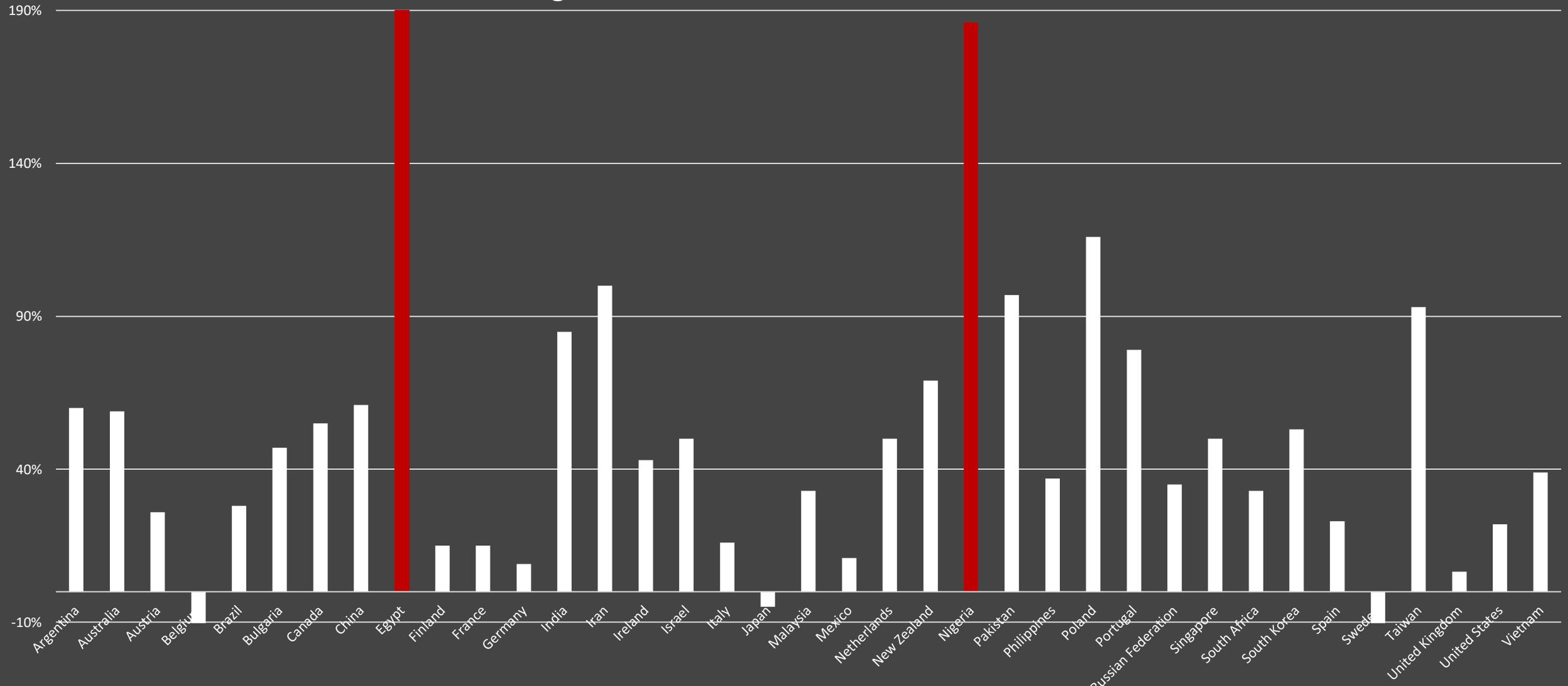
Only Belgium, Japan and Sweden report a (small) decline

Countries (x-axis): Argentina, Australia, Austria, Belgium, Brazil, Bulgaria, Canada, China, Egypt, Finland, France, Germany, India, Iran, Ireland, Israel, Italy, Japan, Malaysia, Mexico, Netherlands, New Zealand, Nigeria, Pakistan, Philippines, Poland, Portugal, Russian Federation, Singapore, South Africa, South Korea, Spain, Sweden, Taiwan, United Kingdom, United States, Vietnam

Y-axis: -10%, 40%, 90%, 140%, 190%

Country Overview Table

	Population	GDP ($, millions)	GDP (€, millions)	Internet Population	Internet Penetration (%)	Number of Scams	Increase in Scams	Scams per 1000 pop	Estimate value Lost (€)	Amount Lost per Capita	Amount Lost per Case
Argentina	45.376.760	$ 383.067	€ 324.303	41.586.960	92%	12966	60%	0,3	€ 6.205.486	0,14	€ 478,60
Australia	25.687.040	$ 1.330.901	€ 1.126.736	21.711.706	85%	444164	59%	17,3	€ 531.802.033	20,70	€ 1.197
Austria	8.917.200	$ 428.965	€ 363.161	7.920.226	89%	18780	26%	2,1	€ 22.536.000	2,53	€ 1.200
Belgium	11.556.000	$ 515.333	€ 436.279	10.857.126	94%	29002	-14%	2,5	€ 36.400.000	3,15	€ 1.255
Brazil	212.559.410	$ 1.444.733	€ 1.223.106	150.457.635	71%	125.410.052	28%	590	€ 438.104.700	2,06	€ 3,49
Bulgaria	6.927.290	$ 69.105	€ 58.504	4.663.065	67%	7300	47%	1,1	€ 7.884.000	1,14	€ 1.080
Canada	38.005.240	$ 1.643.408	€ 1.391.303	35.477.625	93%	56000	55%	1,5	€ 62.329.497	1,64	€ 1.113,03
China	1.402.112.000	$ 14.722.731	€ 12.464.211	904.000.000	64%	2119000	61%	1,5	€ 2.616.965.000	1,87	€ 1.235
Egypt	102.334.403	$ 363.069	€ 307.373	49.231.493	48%		190%				
Finland	5.530.719	$ 271.234	€ 229.626	5.225.678	94%	18837	15%	3,4	€ 23.700.000	4,29	€ 1.235
France	67.391.580	$ 2.603.004	€ 2.203.694	60.421.689	90%	46173	15%	0,7	€ 161.605.500	2,40	€ 3.500
Germany	83.240.520	$ 3.806.060	€ 3.222.197	79.127.551	95%	320323	9%	3,8	€ 3.091.757.596	37,14	€ 9.652
India	1.380.004.390	$ 2.622.984	€ 2.220.609	560.000.000	41%	120.000.000	85%	87	€ 21.274.800.000	15,42	€ 177
Iran	83.992.950	$ 191.718	€ 162.308	67.602.731	80%		100%				
Ireland	4.994.720	$ 418.622	€ 354.404	4.453.436	89%	7818	43%	2	€ 75.810.000	15,18	€ 9.696
Israel	9.216.900	$ 401.954	€ 340.293	7.002.759	76%	8377	50%	0,9			
Italy	59.554.020	$ 1.886.445	€ 1.597.058	54.798.299	92%	77621	16%	1,3	€ 156.600.000	2,63	€ 2.017
Japan	125.836.020	$ 5.064.873	€ 4.287.903	118.626.672	94%	40581	-5%	0,3	€ 216.840.000	1,72	€ 5.343
Kenya	53.771.300	$ 98.843	€ 83.680	46.870.422	87%				€ 251.600.000	4,68	
Malaysia	32.366.000	$ 336.664	€ 285.019	26.353.017	81%	11511	33%	0,4	€ 56.802.754	1,76	€ 4.934
Mexico	128.932.750	$ 1.076.163	€ 911.076	89.000.000	69%	5500000	11%	42,7	€ 385.861.536	2,99	€ 70
Netherlands	17.441.140	$ 912.242	€ 772.301	16.383.879	94%	120.696	1	6,9	€ 80.500.000	4,62	€ 667
New Zealand	5.084.300	$ 212.482	€ 179.887	4.351.987	86%	20120	69%	4,0	€ 21.658.444	4,26	€ 1.076
Nigeria	206.139.590	$ 432.294	€ 365.978	126.078.999	61%	61501	186%	0,3	€ 10.747.469	0,05	€ 175
Pakistan	220.892.330	$ 263.687	€ 223.236	71.608.065	32%	94227	97%	0,9	€ 27.944.560	0,26	€ 297
Philippines	109.581.090	$ 361.489	€ 306.036	79.000.000	72%	1738	37%	0,0			
Poland	37.950.800	$ 594.165	€ 503.018	29.757.099	78%	7622	116%	0,7	€ 8.231.760	0,80	€ 1.080
Portugal	10.305.564	$ 231.256	€ 195.780	8.015.519	78%	1347	79%	0,1	€ 1.334.877	0,07	€ 991
Russian Federation	144.104.080	$ 1.483.498	€ 1.255.924	116.353.942	81%	5330000	35%	37,0	€ 1.740.503.550	12,08	€ 327
Saudi Arabia	34.813.870	$ 700.118	€ 592.717	31.856.652	92%	6595		0,2	€ 49.200.682	1,41	€ 7.460
Singapore	5.685.810	$ 339.998	€ 287.841	5.173.907	91%	14236	50%	2,5	€ 126.859.106	22,31	€ 8.911
South Africa	59.308.690	$ 301.924	€ 255.607	32.615.165	55%	27928	33%	0,5	€ 79.231.777	1,34	€ 2.837
South Korea	51.780.580	$ 1.630.525	€ 1.380.397	49.234.329	95%	208605	53%	4,0	€ 387.597.021	7,49	€ 1.858
Spain	47.351.570	$ 1.281.199	€ 1.084.659	42.961.230	91%	42610	23%	0,9	€ 42.245.155	0,89	€ 991
Sweden	10.353.440	$ 537.610	€ 455.139	9.653.776	93%	145333	-11%	14,0	€ 179.486.667	17,34	€ 1.235
Switzerland	8.636.900	$ 747.969	€ 633.228	8.066.800	93%	10694		1,2	€ 276.695.415	32,04	€ 25.874
Taiwan	23.570.000	$ 668.510	€ 565.958	19.798.800	84%	23054	93%	1,0	€ 94.345.090	4,00	€ 4.092
Turkey	84.339.070	$ 720.101	€ 609.635	69.107.183	82%	1938900		23,0	€ 1.136.195.400	13,47	€ 586
United Kingdom	67.215.290	$ 2.707.744	€ 2.292.366	63.544.106	95%	875622	6,5%	13,0	€ 2.001.225.772	29,77	€ 2.285
United States	329.484.120	$ 20.936.600	€ 17.724.850	313.322.868	95%	2263502	22%	6,9	€ 2.815.798.425	8,55	€ 1.244
Ukraine	44.134.693	$ 155.582	€ 131.715	40.912.381	93%	352000		7,98	€ 115.104.000	2,61	€ 327
Vietnam	97.338.580	$ 271.158	€ 229.562	68.541.344	70%	76155	39%	0,78	€ 197.006.980	2,02	€ 2.587

We blocked 980 million scam sites in 2021 alone

An interview with Kalin Chih, Senior Product Manager at Trend Micro

Can you tell us a bit about Trend Micro?

Trend Micro is a global leader in cybersecurity which has provided consumers, enterprises, and governments with security solutions for over 30 years. The company currently has more than 6,700 employees across 65 countries, providing the world's most advanced global threat research and intelligence.

Trend Micro is one of the few cybersecurity firms focusing on scams, why?

Our mission is to simplify and secure your connected world. That's why we've released Trend Micro Check, a free online tool for identifying scams. **Trend Micro Check** deploys a wide range of anti-scam capabilities to keep you safe online, including detecting fraudulent websites, texts, emails, and phone calls. It blocks deceptive ads, prevents malware, and alerts users to potential identity theft.

During the Covid-19 pandemic, the number of online scams increased significantly. Since the beginning of 2021 Trend Micro has helped businesses and individuals block over **980 million online scam websites**. The top three most common scam types were dating scams, insurance fraud, and shopping scams. Additionally, Trend Micro blocked over 2.4 billion scam and phishing emails. The top three scam email types were package delivery phishing, bitcoin sextortion scam, and cloud service phishing. Ransomware attacks dramatically increased in August 2021. According to our threat research analysts, there has been a rising number of scams spread through social media – including fake accounts and scam ads.

Online scams are the biggest threat that consumers and businesses face. To improve our AI models, we have partnered with **FLOW AI Data Service**, who train physically-challenged individuals to work in the security industry as professional data annotation specialists. By offering high-quality data processing services, they help us enhance our anti-scam algorithms. Likewise, we cooperate with **ScamAdviser.com** to enhance our data and improve our algorithm. We are excited to partner with ScamAdviser to fight scams together!

Kalin Chih,
Senior Product Manager
Trend Micro

Join us at the Global Online Scam Summit!


SCAMADVISER

Global Online Scam Summit

Presents

TURNING THE TIDE ON CYBERCRIME

Powered by

APWG.EU   SCAMADVISER   GLOBAL CYBER ALLIANCE

All findings will be presented at the Summit. Register for free at: www.globalonlinescamsummit.org
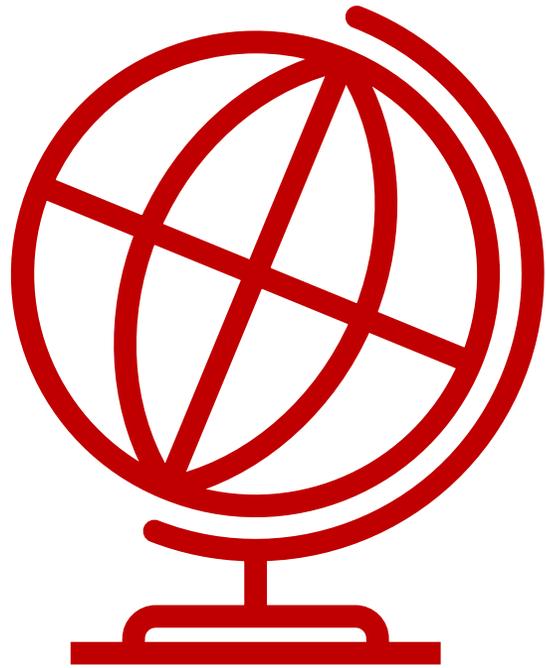
ANALYSIS PER COUNTRY

Argentina reported an increase in scams from 60 to 500%

As scam reporting is not centralized, each region has its own statistics

There are several organizations focusing on cybercrime in Argentina. Consumers can report a cyber crime to the local police station, the municipality, the state or they can contact the office of the Attorney General who has a special cybercrime fiscal unit called **Unidad Fiscal Especializada en Ciberdelincuencia** (UFECI).

For IT related crimes, consumers can also email the federal police. There is a special unit called the **National Cybercrime Directorate**. The CERT is part of this organization.

It is also possible to report online fraud to the **National Directorate for Consumer Defense** (Defensa de las y los consumidores) who will refer the consumer to the appropriate body.

The **Argentine Association for the Fight Against Cybercrime** (AALCC) is a non-profit association whose main objective is to eradicate computer crimes and crimes committed through the Internet by providing guidance, training, and prevention.

As a result, the number of scams reported differs strongly by region and organization. The UFECI, led by prosecutor Horacio Azzolin, reported 2,369 cases in 2019 and 11,396 in 2020, an increase of 381%. AALCC received 1,570 report, an increase of 65%.

The Buenos Aires Ombudsman Office also reported a growth of 60% compared to the year before while the municipality Consumer Defense directorate in Parana reported a growth of 500% with amounts lost averaging 50,000 to 60,000 pesos.

The rise of online fraud is mainly caused by the Covid-19 pandemic and the sharp rise of e-commerce. The most common scams were online purchases via social media where the victim did not receive the ordered products and phishing via telephone calls where the offender claimed to represent government organizations.

cibercrimen.org.ar/2020/12/24/estadisticas-ano-2020-completo/
fiscales.gob.ar/ciberdelincuencia/la-unidad-fiscal-especializada-en-ciberdelincuencia-dimensiono-el-crecimiento-de-los-delitos-informaticos-en-su-informe-de-gestion-2020/

Share of Reports

Category	
child pornography	
Grooming	
others	
Public Illegitimate Image	
identity theft	
Threats	
slander	
cybebullyng	
Online extortion	
Phishing data theft	
Fraud	

0,00%   5,00%   10,00%   15,00%   20,00%

Key Statistics:

Population:	45.4 million
Internet:	92%
# of Scams:	12,966 (60%)
Scams / 1,000 :	0.3
Money lost:	€ 6.2 million
Per capita:	€ 0.14
Per report:	€ 479

Key Organizations:

MINISTERIO PÚBLICO FISCAL

AALCC

Argentina.gob.ar

Hope Funds, the largest scam in Argentina's history

The damage reached 1,500 million pesos; more than 300 victims reported it in court.

Blaksley with Roger Federer and Adolfo Cambiaso

Hope Funds was dedicated to taking 'mutual contracts'; investors gave their money under the promise of returns of more than 10% of their capital. The funds were however used to pay 'interest' to existing clients and in marketing to lure new victims to 'invest'.

In the end, Blaksley, The "Argentine Madoff", stopped paying interest. His offices proved to be deserted. Slowly the police began receiving the first complaints which ended with more than 300 victims filing reports and claiming losses of more than 1.5 billion pesos.

In 2020, the court case against Enrique Blaksley Señorans and 15 other people started. The accusation was that of having led a gang that carried out the most important financial scam in Argentine history. Blaksley is accused of having put together a complex network of 42 Argentine companies, 3 real estate trusts and 66 foreign organizations headed by the firm Hope Funds, which promised to make savers rich.

The company used well-known brands to build business credibility and socialites. His victims were businessmen, celebrities as well as ordinary people.

Blaksley with Serena and Venus Williams

Together with Covid-19, bushfires increased scams in Australia

Australia reported an increase of 59% in scam reports and a 23% growth in money lost

The **Australian Competition & Consumer Commission** (ACCC) has been monitoring scams for 12 years together with **ScamWatch**. It witnessed a sharp rise in the number of scams. This was not only due to the COVID-19 crisis but also to the huge number of bushfires plaguing the country.

In 2020, ACCC reported a loss of 850 million AU$ and over 444,000 scam reports to Scamwatch and other government agencies, banks and payment platforms. Previous research done by ACCC discovered that only 13% of scam victims filed reports with ScamWatch.

Scammers set up fake charity scams in response to the bushfires and took advantage of pandemic-related incentive schemes available in Australia. Phishing reports grew by 75%. Other scams grew even more. Threat-based scams, which typically involve scammers threatening victims with arrest, deportation, legal action or excessive fees unless a sum of money is paid, increased by 140%. Identity theft reports increased by 84%.

The most popular contact methods remained phone (47%), email (22%) and text messages (15%). 25- to 34-year-old reported the largest number of scams (20%) while 65+ lost the most money (24%).

Key Statistics:

Population:	26,6 million
Internet usage:	85%
# of Scams:	444,164 (59%)
Scams / 1,000 :	17,3
Money lost:	€ 532 million
Per capita:	€ 20.70
Per report:	€ 1,197

Key Organizations:

ACCC AUSTRALIAN COMPETITION & CONSUMER COMMISSION

SCAMWATCH

Amount lost (AU$, mil)

Unexpected prize & lottery scams
Identity theft
Health & medical products
Classified scams
Online shopping scams
Remote access scams
Threats to life, arrest or other
False billing
Dating & romance
Investment scams

0 10 20 30 40 50 60 70

Number of reports

Unexpected prize & lottery scams
Investment scams
Classified scams
Remote access scams
Hacking
False billing
Online shopping scams
Identity theft
Threats to life, arrest or other
Phishing

0 10 20 30 40 50

We need to keep adapting

An interview with Jayde Richmond and Alex Meaney, of the Australian Competition & Consumer Commission

How was 2020 for ScamWatch Australia?

Most of our states are still in lockdown. Physical crime is down as a result, but we are receiving more complaints about scams than ever before and this trend seems to be increasing in 2021. The number of phishing scams is skyrocketing. We had several data breaches last year and the information harvested in now being misused by cybercriminals.

At the moment Flubot is hitting us. Since August 2021, many Australians have been getting Flubot scam text messages about missed calls, deliveries, leaked photo albums and more. In the month after this scam was first reported, ScamWatch received over 9,500 reports. In some variants, victims receive messages asking them to click on a link to download an app to track or organize a time for a delivery or hear a voicemail message. However, these messages later turned out to be fake as there is no delivery or voicemail, and the app is really a malicious software which steals credentials.

Investment scams increased by 162%. We saw a strong growth in questionable cryptocurrency sites offering huge daily returns and forex trading. Men aged 50 and over are the most impacted demographic. 96 million AU$ were lost in 2020. Some investment scams have combined with dating and romance scams. These may start as romance scams but turn into investment scams as the "lover" convinces the victim to invest in a "sure thing". We are also continuing to see business email compromise and fake invoices scams, and remote access/tech support scams. We work together with remote software companies and Microsoft to combat these.

The "good" news is that online shopping and charity scams are stable, and the amount of money being lost, relative to the number of scams, seems to be decreasing.

Jayde Richmond
Director Consumer
Strategies & Engagement

What is your biggest challenge fighting scams?

One of your biggest challenges is getting consumers to report scams. Among scam victims, only 12% - 13% report the scam. Overall, consumers are more likely to report scams to the banks. ScamWatch is the second most used government reporting agency after the police.

What is ScamWatch doing to protect consumers?

We continue to focus on building consumer awareness. Our current message is simple and focused on Flubot: "Think 3D's : DON'T click links, DON'T download & DELETE!". We use both social as well as mass media. Although we see awareness increasing, scams keep changing.

We are increasingly working together with law enforcement and other agencies such as the Australian Financial Regulation Commission, banks and telecom operators to improve security and raise the costs of scamming. New legislation has made banks more responsible for protecting Australian consumers. A joint effort with Australian job boards has resulted in a sharp drop in typical job and unemployment scams.

We are also increasingly cooperating with social media and online platforms such as Facebook and Google. These companies could improve by taking more responsibility and using their own data to protect consumers and disrupt the work of scammers.

Finally, we are also sharing data increasingly internationally, such as with the Federal Trade Commission to identify scams faster and facilitate the intervention of law enforcement.

Alex Meaney
Assistant Director

In Austria cybercrime increased by 26.3%

Consequently, Austria will double its cybercrime police unit within the next year

Online scams can be reported to the local, state or federal police . On the federal level, a separate unit, the Cyber Crime Competence Center (C4), has been set-up. C4 focuses especially on cyber crimes such as hacking and DDoS attacks. Online scams and child pornography are also part of its assignment. Consumers can report crime directly to C4 via **against-cybercrime@bmi.gv.at**

Since 1997 **OIAT** (the Austrian Institute for Applied Telecommunication) has launched several initiatives to make the Internet a safer place. OIAT offers a trust seal for reliable online stores, maintains **Saferinternet.at** with tips and tricks on how to use the Internet safely, runs **Watchlist Internet** with a manually vetted list of malicious and dubious websites and **Fake-Shop Detector**, a browser extension to check sites using artificial intelligence. In 2020, OIAT reported 3,182 fake webshops to the Austrian public.

The number of cyber crime reports increased from 28,439 in 2019 to 35,915 in 2020 - an increase of 26.3%. The largest type of cybercrime was Internet fraud, which reached a new high of 18,780 reports (compared to 16,831 in 2019). Despite the considerable increase, the percentage of solved cases remained almost constant at 33.4%.

The Covid-19 pandemic has shifted many areas of daily private and professional life to the Internet. This has also had significant consequences in terms of cybercrime. At the beginning of the pandemic, there was a sharp increase in fraudulent websites (target: phishing, spreading malware) following the re-registration of several thousands' domains. Due to social distancing, there was also an increase in scams, such as Love Scam or the so-called Stranded Travelers. In fake stores, as well as on regular platforms, there was an increase in fraud.

■ Cybercrimes Reports   ■ Cybercrimes Solved
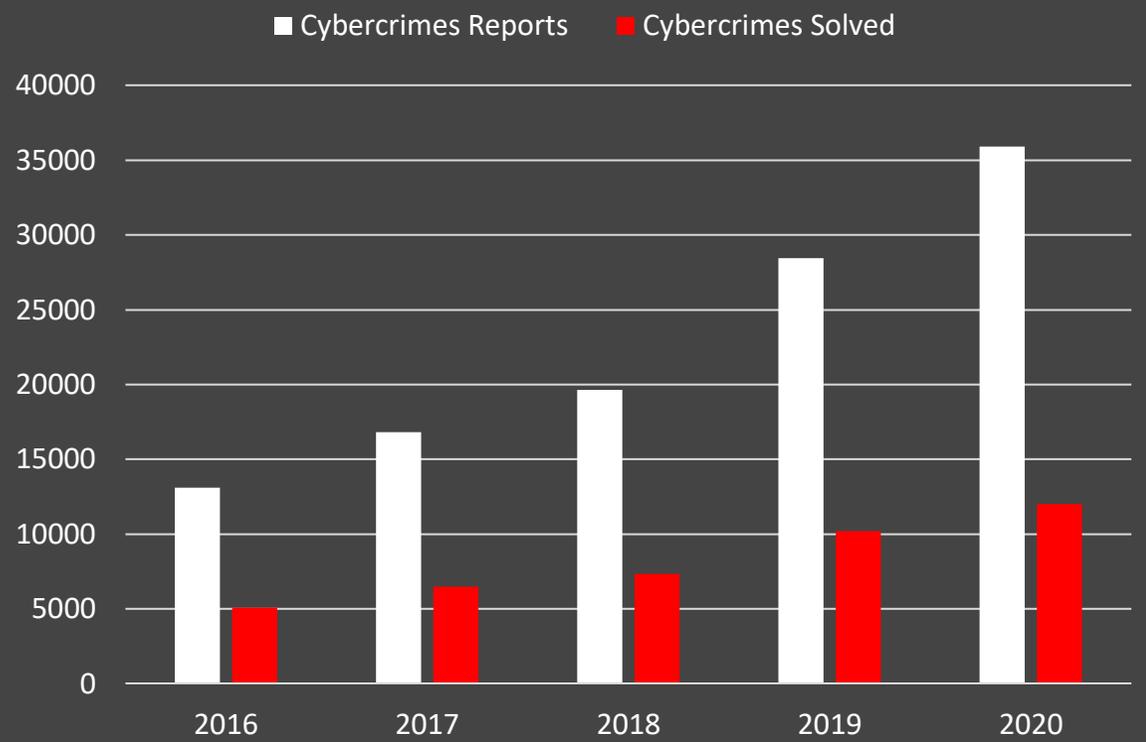
Key Statistics:

Population:	8.9 million
Internet:	89%
# of Scams:	18,780 (26%)
Scams / 1,000 :	2.1
Money lost:	€ 36.4 million
Per capita:	€ 2.53
Per report:	€ 1.200*

Key Organizations:

Bundesministerium Inneres
Bundeskriminalamt

oiat

Belgium report a decline of 14% in online/offline scams

However, the number of reported phishing cases grew to 7,424, nearly three times as much as in 2019

The Centre for Cybersecurity Belgium (CCB) is the national authority for cybersecurity in Belgium. The CCB was established by the Royal Decree of 10 October 2014 under the authority of the Prime Minister. The CCB supervises, coordinates and monitors the application of the Belgian cyber security strategy. Through information exchange, companies, the government, providers of essential services and the population can protect themselves appropriately. CERT.be is an operational unit of CCB.

CCB supports several initiatives to prevent and fight online scams. SafeOnWeb.be helps consumers to be safe online. It also offers an email address where consumers can report phishing emails. This has proved to be a huge success. In 2020 more than 12,000 emails per day were received by suspicious@safeonweb.be (see next page).

Belgians can report online scams via several channels. Online fraud can be reported to both the local police and centrally on Police On the Web. If reported online, the report is handed over to the local police force. Online fraud is not yet reported as a separate crime by the Belgium Police. There is also currently no regional or national police team focusing on online fraud.

Belgians (both consumers as well as businesses) can also report misleading practices, fraud or swindles to Report Belgium. The information is passed along to the appropriate authority who subsequently analyzes the report and may carry out a further investigation. Report Belgium is a joint venture of the Federal Agency for the Safety of the Food Chain, the Federal Agency for Medicines and Health Products, the FPS ELSD, the Federal Police, the FPS Finances, and the Federal Public Service (FPS) Economy. The latter is also the technical manager of the system.

There is little data available on the amount lost in scams. In one BEC case it was reported that € 75 million were lost.

statista.com/statistics/535525/fraud-cases-in-belgium/
stat.policefederale.be/criminaliteitsstatistieken/rapporten/

Registered cases of fraud in Belgium from 2008 to 2020

Year	Cases
2008	11190
2009	12818
2010	13050
2011	12528
2012	20204
2013	19453
2014	20333
2015	21888
2016	22053
2017	23717
2018	28835
2019	34030
2020	29002

Key Statistics:

Population:	11.6 million
Internet:	94%
# of Scams:	29,002 (-14%)
Scams / 1,000 :	2.1
Money lost:	€ 36.4 million
Per capita:	€ 3.15
Per report:	€ 1,255

Key Organizations:

CENTRE FOR CYBER SECURITY BELGIUM

Safeonweb.be

economie FOD Economie, K.M.O., Middenstand en Energie

REPORT

POLICE ON WEB www.police-on-web.be

Relax

And think twice before clicking on a link.

Recognise suspicious messages in time and send them to suspicious@safeonweb.be

CCB checks the links and attachments of the forwarded messages. The suspicious URLs from these emails are sent to Belgium Internet Service Providers to block the domains and to Google SafeBrowsing and Microsoft SmartScreen to warn visitors about malicious websites. In 2020, 3,200,000 messages were forwarded to suspicious@safeonweb.be. From 1st January 2021 to 6th July 2021, more than 2,332,000 emails were received, 551,014 unique URLs analyzed, and 26,292 domains tagged as malicious. Despite the fact that the process is fully automated, the number of false positives has been minimal.

In 2020, 59% of Brazilians suffered from a financial scam

Online fraud incidents grew by 28% compared to 2019 and 2.7 billion R$ (€438 million) were lost

In Brazil, scam fighting is organized in a decentralized way. A growing number of states have police teams focusing on cybercrime. There is also a federal cybercrime team.

Consumidor.gov.br, set-up by SENACON, the national consumer secretariat, allows consumers to file a complain about a company's service. In 2020 1,2 million complains were received, 99% were answered by the company complaint about. However, consumers can only complain about participating companies. For scams, consumers are directed to local consumer protection agencies, called **PROCON**, public defenders, special civil courts, and other bodies.

There are nearly 1000 **PROCON's** (consumer protection agencies) in Brazil. The PROCON's are funded either on the state or on the municipality level. A non-profit initiative to help customers identify scams and fake websites has also been set up; this is called "**Posso Confiar**" (or Can I Trust?). **ReclameAqui** is a commercial initiative which allows consumers to rate companies and it is the most popular review website in Brazil.

Cert.br reported 665,079 cybercrime incidents in 2020. 4,6% of these were related to online fraud and phishing. Whatsapp and social media are by far the most popular platforms on which scammers operate. According to the Brazilian Federation of Banks (Febraban), in 2020 the number of phishing attempts exploded with 340%.

Next to phishing, the most popular scams are: paying for but not receiving the product or service, receiving a product or service different from what sold, credit/debit card cloning, advance payment scams, and false billing. 56% of the people from the lower-middle class are being scammed. Upper class citizens are scammed slightly less, 44%. 51% of the victims are women, 49% man.

"Brazil is maybe on of the most complex ecosystem for criminals in the world. It's a country as huge as a continent, with a highly complex justice system that does not allow to arrest anyone, and a large portion of the population that is poor and marginalized. It's kind of a perfect storm for cyber scammers. "

Fabio Ramos
CEO Axur

Key Statistics:

Population:	212,6 million
Internet:	71%
# of Scams:	125 Mill. (28%)
Scams / 1,000 :	590
Money lost:	€ 438 million
Per capita:	€ 2.06
Per report:	€ 3,49

Key Organizations:

19 Cybercrimes Police Stations

PROCON   **ReclameAQUI**

cert.br/stats/incidentes/2020-jan-dec/fraude.html
site.cndl.org.br/seis-em-cada-dez-consumidores-sofreram-algum-tipo-de-fraude-financeira-nos-ultimos-12-meses-aponta-cndlspc-brasil/

We have to educate the youth in order to beat cybercrime

An interview with Érico Rodrigues de Melo, President of PROCON Paulstas

Can you explain what PROCON is?

All Brazilian states have at least one PROCON office. PROCON is responsible for guiding consumers in their complaints and for providing them with information about theirs rights. Municipalities can set-up a PROCON as well. While the organization is decentralized, there are several coordinated efforts such as a "Do Not Call Me" register and a central complain site called **Consumidor.gov.br**.

Can you describe the "scam situation" in Brazil

Social media platforms are extremely popular in Brazil. A great number of scams take place here. In 2020 we had a huge issue with unsolicited loans where a company deposited money into a person's bank account without any request. This impacted particularly elderly people who often did not know how to check their bank accounts online and instead tended to do their transactions by physically going to the bank. As a result, in many cases, they were unable to return the money.

How can we best fight online scams?

A recent law has increased the penalty for online scams from 4 years and 8 months upward. The penalty can be further increased by 1/3 if the targets are vulnerable people.

We also have to increasingly educate the youth. My PROCON has developed an online "muppet show" which is focused on explaining the dangers of the Internet to young children in a language they can understand.

Finally, platforms like Facebook and Google have to take more responsibility. For example, Whatsapp is being largely misused to install malware on phones. We are in a continuous discussion with them on how they can improve their protection of consumers. Likewise, we are battling to enforce the imposition of counter advertisement, i.e. social media and companies in which scams are perpetrated could also be punished through counter advertisement and/or financing of educational campaigns for consumers in the digital environment.

Érico Rodrigues de Melo
President PROCON Paulstas

BEC is the number 1 scam in Bulgaria

This is followed by Investment Fraud and Romantic Data Schemes

Several organizations are involved in fighting cybercrime in Bulgaria. The General **Directorate Combating Organized Crime (GDCOC),** part of the Bulgarian Ministry of Interior has set-up a special **Cybercrime Police** unit consisting of 40+ officers who tackle local and transnational organized criminal structures related to computer crimes or crimes committed in or through computer networks and systems.

The national computer emergency response team (CERT) helps its users to reduce the risks of information security incidents and to resolve incidents which have already occurred. There is also a national Computer Security Incident Response Team (NCSIRT), and sector-level Computer Security Incident Response Teams (SCSRITs) established by the State e-Government Agency. The SCSIRTs are set up locally for various sectors (i.e., energy, transport, banking, financial market infrastructure, health, and digital) in compliance with the instructions of European Union Cybersecurity Agency (ENISA). They coordinate their activities with the national CERT.

According to the NCSIRT, 2,100 cyber incidents have been registered in 2020. This is an increase of 9% compared to 2019. The highest percentage of registered incidents was due to fraud (47%), followed by malware (38%).

On **Cybercrime.bg**. any interested party was able to alert GDCOC of online fraud or scams. Since March 2021, this functionality has been removed. Most online fraud is now reported directly to the office of the Cybercrime Team in Sofia (30%). Reports can also be made via e-mail (30%). The unit receives approximately 20 reports daily.

Should personal data be involved, complains can be submitted directly to the Bulgarian Commission for Personal Data Protection. In case of consumer protection related cases, complaints can be submitted to the Bulgarian Commission for Consumer Protection.

The most common scams reported to the Cybercrime team are:

1) **Business Email Compromise (BEC)**: BEC scams mainly originate in Nigeria. The scammers use phishing to gain access to the mail server. Amounts lost range from €50,000 to more than €2.5 million.

2) **Investment and crypto frauds**: These type of scams are mainly run from Israel. Bulgarian consumers are convinced by phone and social media to invest small amounts of money, usually around €50. The investment quickly shows high returns after which the victim is convinced to invest larger amounts. Amounts lost range up to €50.000 and more.

3) **Romantic dating scams**: A large number of scammers from Benin are targeting Bulgarian women aged 60 to 70. The scammer often plays the role of an American soldier. Amounts lost range up to €60.000 .

The Cybercrime Police receives between 20 and 150 reports daily.

Key Statistics:

		Key Organizations:
Population:	6.9 million	
Internet:	67%	Cybercrime Police
# of Scams:	7,300 (47%)	
Scams / 1,000 :	1.1	
Money lost:	€ 7.8 million	CERT.BG
Per capita:	€ 1.14	
Per report:	€ 1.080*	

Canadians lose the most money in Romance Scams

Only 5% of Canadians file a fraud report with the CAFC when they are victims of scams

Online scams can be reported to the **Canadian Anti-Fraud Centre (CAFC),** managed by the Royal Canadian Mounted Police, the Competition Bureau Canada, and the Ontario Provincial Police.

The CAFC reported **56,000 incidents** of fraud in 2020, compared to 36,000 in 2019. The amount of money lost also increased, with a reported **$92.4 million** in losses from 2020's top 10 list compared to $81.2 million lost according to the 2019 list.

Reports of phishing scams decreased (from 5,053 to 3,672), as did personal information scams (from 7,642 to 6,649). However, the number of reports for other types of scams increased, including extortion (from 10,278 to 17,390), merchandise fraud (from 2,452 to 3,354), and job fraud (1,702 to 2,297). Romance scams, meanwhile, emerged as the new top scam in terms of losses (from $18.3 million in 2019 to $18.5 million in 2020), despite a fall in the reported number of incidents. Losses reported from investment scams also swelled from $10.7 million in 2019 to $16.5 million in 2020.

The **Canadian Competition Bureau** is the driving force behind the **Fraud Prevention Forum,** a group of 60 private sector firms, consumer and volunteer groups, government agencies and law enforcement organizations, who are committed to fighting fraud aimed at consumers and businesses. Each March the forum organizes a Fraud Prevention campaign. The organization also maintains the Little Black Book on Scams.

CIRA, the **Canadian Internet Registry Authority**, fights scams by offering a free DNS service to protect consumers from malware and phishing, a firewall solution for companies and cybersecurity awareness trainings for companies.

Fraud type	Reports	Victims	Lost ($CA)
Romance	899	620	18.5
Investment	501	428	16.5
Spear phishing	1,049	525	14.4
Extortion	17,390	6,689	12.5
Merchandise	3,354	2,728	8.7
Service	2,009	1,241	8.5
Victim vendor	2,320	1,478	4.2
Prize	754	240	3.5
Job	2,297	1,035	2.6
Bank investigator	835	340	3
Identity fraud	16,970	16,970	N/A
Personal information	6,649	4,386	N/A
Phishing	3,672	1,167	N/A

Key Statistics:
Population: 38 million
Internet: 93%
# of Scams: 56,000 (55%)
Scams / 1,000 :   1,5
Money lost: € 62.3 million
Per capita: € 1,64
Per report: € 1,113

Key Organizations:

Education and the right tools, can keep cybercrime at bay

An interview with Mark Gaudet, General Manager of Cybersecurity & DNS Services at the Canadian Internet Registry Authority

How would you describe the cybercrime situation in Canada

The cybercrime landscape in Canada has shifted significantly due to the pandemic. While it's clear that cyber attacks were on the rise before the pandemic, the sudden shift to remote work was a massive opportunity for cyber criminals. We saw an increase in attacks due to the pandemic, including COVID-19 themed attacks (phishing attacks posing as COVID-19 test results or contact tracing apps, etc.).

What is CIRA doing to fight scams and cybercrime? How is it working together with other organizations?

About five years ago, CIRA decided to leverage its years of experience managing and protecting the DNS for the .CA domain to help protect organizations from cybercrime. CIRA DNS Firewall helps identify and protect organizations against cyber attacks; CIRA Anycast DNS provides protection against DDoS attacks; and CIRA Cybersecurity Awareness Training helps employees ensure they are cyber smart.

More recently, we saw that many Canadians were struggling to protect their home networks from scammers and cyber attacks, so we launched CIRA Canadian Shield, a free version of our DNS Firewall.

With the pandemic, there has been a large increase in online commerce that has been accompanied by a similar increase in online fraud targeting consumers and, to a lesser degree, businesses. While our cybersecurity services are very effective in protecting against phishing and malware in their threat feeds, many cybersecurity products do not protect consumers against fake and fraudulent e-commerce sites. To fill that gap, we are integrating the ScamAdviser threat data into all our DNS security products.

Can we win the war on cybercrime, and if so, how?

The war on cybercrime is probably a misnomer as cybercrime, like regular crime, is simply a reality of our society. Tools like CIRA Canadian Shield are one part of the solution. However, the most important steps to take should be focused on training and education. Much like our parents taught us to be street smart, we need to teach our kids, as well as adults, how to avoid scams online.

Mark Gaudet
General Manager Cybersecurity & DNS Services
Canadian Internet Registry Authority

In 2020, China has been cracking down hard on online fraud

361,000 people were arrested for online fraud, an increase of 121% compared to 2019

In 2019, China's new e-commerce law took effect, enhancing the protection of consumers, as merchants must guarantee more transparency and a more careful monitoring of fraudulent practices. The current law is mostly applicable to cases where a victim has lost more than 2,000 RMB (€263). There is no systematic legal recourse for victims who lost a smaller amount.

The **Ministry of Public Security (MPS)** prevents, investigates, and stops criminal activities in general, including online fraud. Chinese citizens can report scams online or call 110 to report the crime directly to the **Cyberpolice** which is part of the MPS.

The National Internet Information Office hosts an **Illegal Information Reporting Center through which companies** and consumers can report incidents online, by phone as well as through apps. The center received 163 million reports; 145 million of these reports were received via major platforms such as Baidu, Alibaba, Tencent. 2.1 million (1,3%) of all reports were related to online fraud.

The **Liewang101猎网平台, platform** also fights online scams in China. It reported a growth of 47% in 2020. On average 9,400 RMB (€ 1,235) was lost. Consumers can report and search phone numbers, domain names and QQ addresses. It is part of Beijing Municipal Public Security Bureau, and it is sponsored by 360.com, an online security company. A similar website is **Black Cat**, where consumers can file all kinds of complaints.

According to the LieWang platform, the most common frauds were gaming scams (17%) where game accounts or assets are offered. Game scams are followed closely by investment schemes (16%). Thirdly were online stores selling fakes or not delivering at all. The most common platforms used for scams were WeChat and twitter-like Weibo.

Reported internet violations 2020

Pie chart values:
- violence/terrorism; 0,90%
- Sensitive data; 1,10%
- Online Fraud; 1,30%
- IP Infringements; 2,20%
- Politics related; 7,70%
- Online Gambling; 9,80%
- Other; 12%
- Adult Content; 61,70%
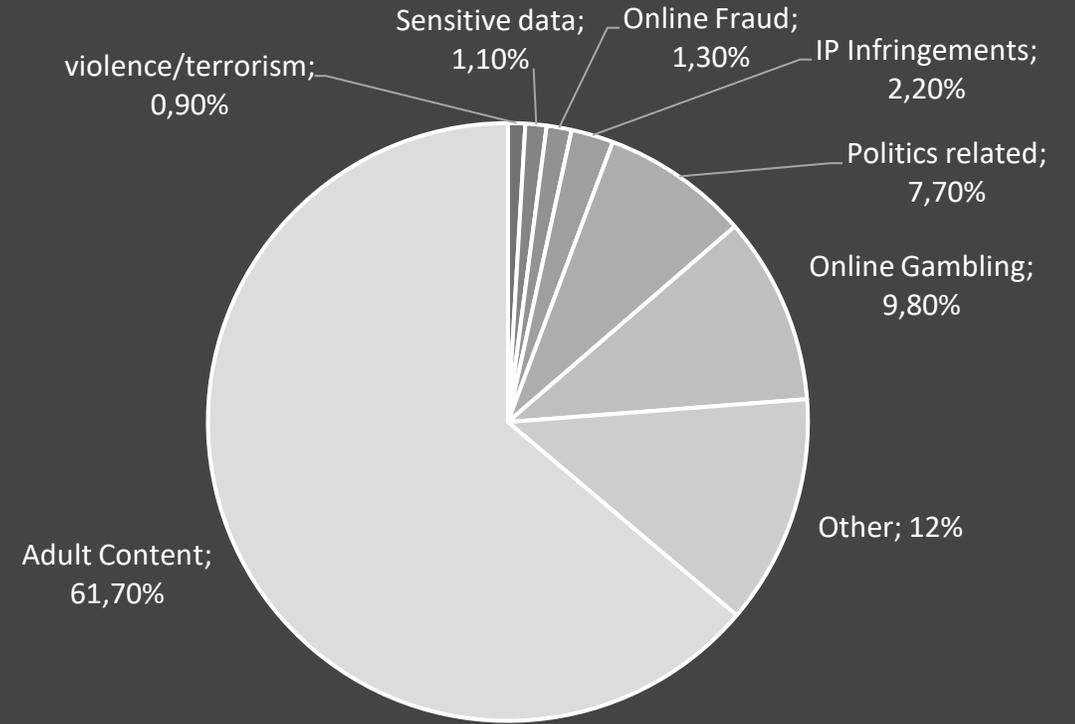
Key Statistics:

Population:	1,402 million
Internet:	64%
# of Scams:	2.1 mil. (61%)
Scams / 1,000 :	1.5
Money lost:	2,616 million
Per capita:	€ 1,87
Per report:	€ 1,235

Key Organizations:

China Cyberpolice

黑猫投诉 新浪旗下消费者服务平台

LieWang Platform

猎网平台

中国互联网 违法和不良信息举报中心 China Internet Illegal Information Reporting Center | 12377 www.12377.cn
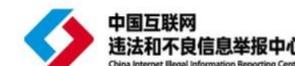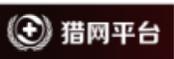
Using big data China prevented a loss of 187.6 billion yuan

Using big data more than 140 million phone calls and 870 million text messages have been intercepted

As of December 2020, 61.7% of China's Internet users said they had not experienced any cybersecurity problems in the past six months, up 5.4% points from March 2020. The proportion of Internet users experiencing all kinds of cybersecurity problems decreased. Specifically, the proportion of Internet users who had suffered from cyber fraud decreased by 4.6% points.

MPS reported that the police across the country cracked 322,000 cases of telecom and online frauds in 2020 (up 61%), arresting 361,000 suspects, an increase of 121%. Additionally, 1.6 million fraudulent websites were blocked. A cumulative loss of at least 187.6 billion yuan (€24.6 billion), involving 8.7 million potential victims, was averted as a result.

The MPS, together with the Cyberspace Administration of China, have launched a big data platform, an app, and a fraud alert hotline to intercept and block fraudulent contents. A total of 140 million phone calls and 870 million text messages involved in fraudulent activities have been intercepted so far.

The country's central bank and telecom regulators and operators have also launched special campaigns to plug loopholes and rectify malpractices to address fraud. MPS plans to continue to invest in big data analysis and special campaigns to crack down on cybercrime.

The Chinese government also increasingly works together with its South-East Asian neighbours, especially Cambodia but also Myanmar, Laos and the Philippines to crack down on cross border scams, such as online gambling, which is illegal in China, but also other kinds of scams.

Types of Cybersecurity Problems

	Mar-20	Dec-20
Personal information leakage	23,3%	21,9%
Cyber fraud	21,2%	16,5%
Devices hacked with trojan horse or other viruses	12,0%	10,8%
Account or password stolen	12,5%	8,2%
None of the above	56,4%	61,7%

Types of Cyber Fraud

Legend: Mar-20, Dec-20

- Bonus winning fraud
- Online part time fraud
- Online shopping fraud
- Fake friend fraud
- Phishing website fraud
- Fake employment information fraud

0,0%   10,0%   20,0%   30,0%   40,0%   50,0%   60,0%
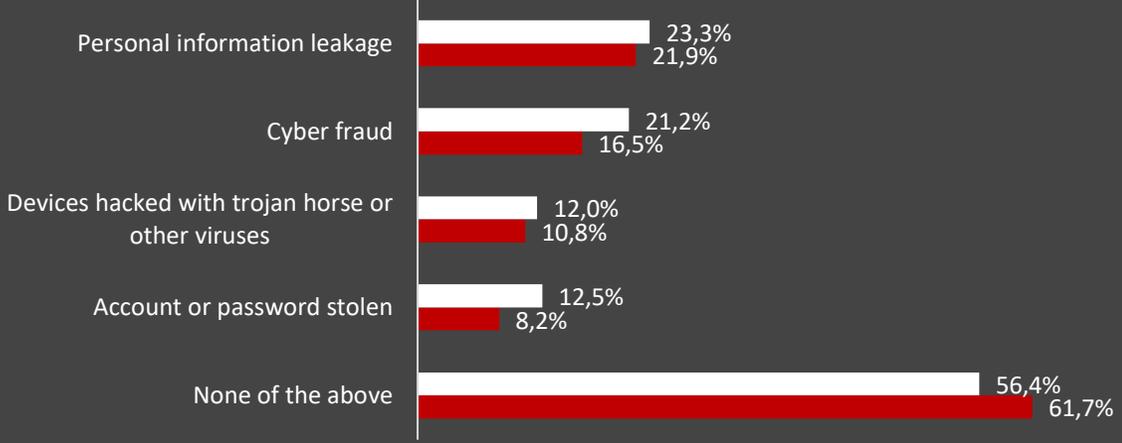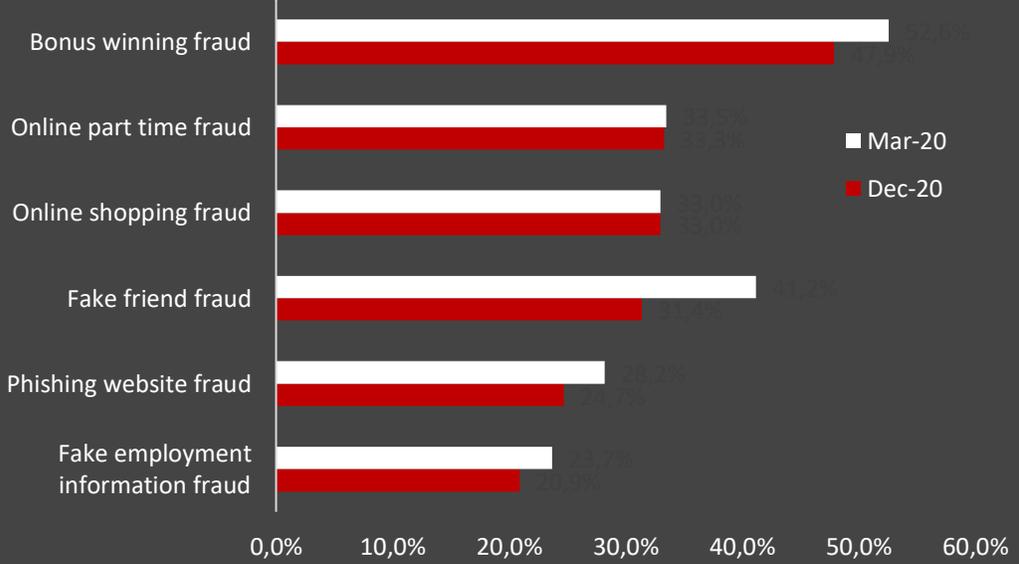
Cybercrime in Egypt has increased by 190%

There are no official statistics about Cybercrime in Egypt

Recently, the Head of the Cabinet's Information and Decision Support Center (IDSC) stated that cybercrime in Egypt has increased by 190% in the recent years, explaining that most of the crimes penetrated websites and altered their homepages and content.

In 2002, The Egyptian Ministry of Interior created a special unit to fight against cybercrime. Its primary role is to provide technical assistance in the detection and investigation of crime wherein the computer is the target, or the means used. The Cyber Crime Unit is made up of police officers.

The Egyptian Public Prosecution has created a special unit to follow-up social media and trace any violation of internal laws.

In 2018 Egypt adopted cybercrime law no. 175. The third part of this law, starting from articles 13 has a long list of offences such as unauthorized access offences and online scams which are punishable by fines and imprisonment.

Another important point is the construction of economic courts in Egypt in 2008. Economic courts in Egypt have jurisdiction over economic issues in both civil and criminal proceedings, including cybercrimes, the stock market, the Central Bank of Egypt, intellectual property, and other matters. These are special courts that examine cybercrimes and online scams.

Consumers can report scams via a special hotline and in person at the headquarters of the Egyptian Ministry of Interior. The most common types of online fraud focused on consumers advance fee scams and phishing scams.

Trend Micro, a company specializing in information security, announced in a recently released semi-annual report that it had addressed 12.4 million email cyber-threats in Egypt in the first half (H1) of 2020. The report also revealed that Trend Micro solutions blocked nearly 1 million URL links, preventing users from accessing them. It indicated that over 235,000 malware attacks were detected in Egypt, and more than 6.8 million malicious mobile applications were found.

Business e-mail compromise (BEC) attacks have also increased by 18%, which can partly be attributed to fraudsters looking to exploit home-based employees more vulnerable to social engineering threats.

Of all the threats that occurred during H1 of 2020, ransomware was a constant feature. Although the number of detected ransomware threats decreased, Trend Micro saw a 36% increase in ransomware families.

Key Statistics:

Population:	102 million
Internet:	41%
# of Scams:	(190%)
Scams / 1,000 :	-
Money lost:	-
Per capita:	-
Per report:	-

Key Organizations:

Despite the language barrier Finland is increasingly targeted

The number of phishing attempts and romantic dating schemes has increased sharply during COVID-19

Finnish consumers can report online scams to the **police**, both locally and online. Finland has a police cybercrime unit as well, which is part of the National Bureau of Investigation. However, this team focusses on bigger cases such as DDOS attacks, BEC and botnets. There is no specialized team for consumer related online fraud.

Consumers can also report scams to the **Finnish Competition and Consumer Authority** (KKV). KKV offers consumer advice in case of disputes both online and by phone. It also works with other organizations such as the **Finnish Financial Supervision Authority** for financial scams, the **Finnish Medicines Agency** for issues regarding drugs, and the **Finnish European Consumer Center** if the purchase has been done in a EU country.

The number of fraud cases, both online and offline, reported to the Finnish Police for 2020 was 18,837. The most common types of fraud were advanced payment (28%) and scams related to the purchase of goods and services (10%). The number of reports is likely to be only a fraction of the total number of scams. According to a survey by insurance company MySafety, more than half a million Finns have been targets of identity theft attempts over the past year. The number of attempts has risen sharply since the start of the pandemic.

The total amount of money lost to scams is not recorded. However, 1,000 Microsoft IT support scams alone were reported and €2.8 million was lost. In the first half of 2021, 900 phishing scams had been reported, having caused € 13.5 million in losses.

RIKU, the national victim support organization, offers free support and advice via phone, chat and online. The organization helps all kinds of victims and works intensively together with volunteers.

Sources: Finish Police Data
yle.fi/uutiset/osasto/news/police_finns_lose_1m_to_online_fraudsters_so_far_this_year/11804957
https://www.stat.fi/til/rpk/2021/01/rpk_2021_01_2021-07-14_tau_001_en.html

Fraud Reported

Bar chart showing Fraud Reported: 2017 ≈ 11,300; 2018 ≈ 12,000; 2019 ≈ 14,500; 2020 ≈ 16,800; 2021-H1 ≈ 17,200
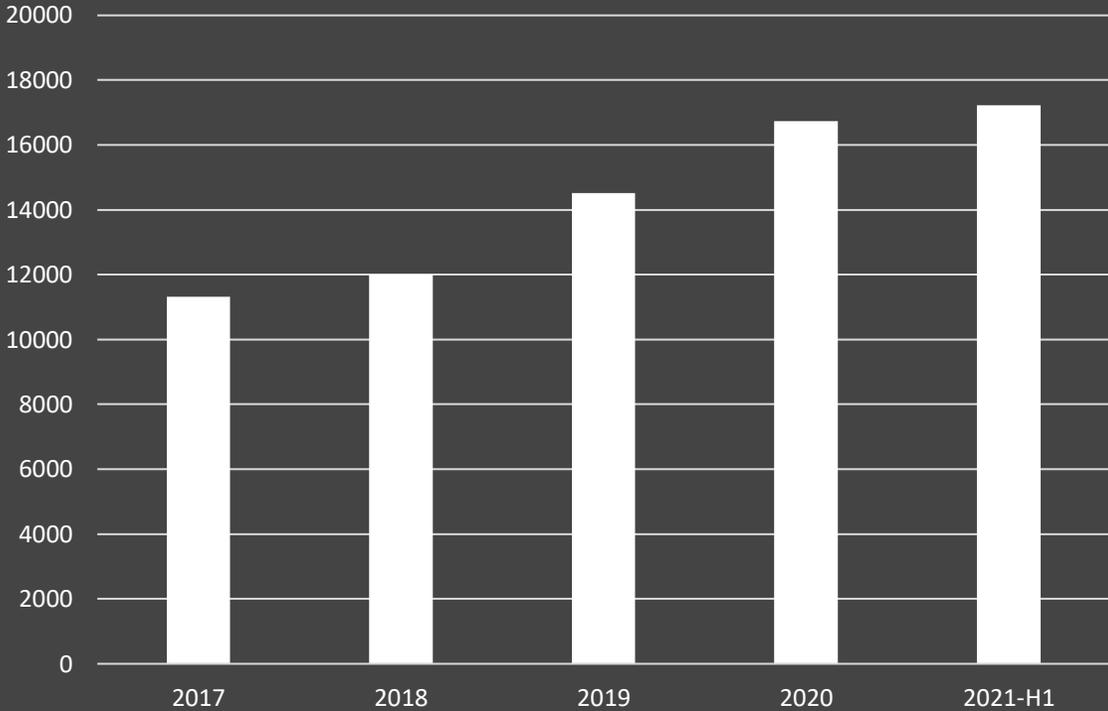
Key Statistics:

Population:	5.5 million
Internet:	94%
# of Scams:	18,837 (15%)
Scams / 1,000 :	3.4
Money lost:	€ 23.7 million
Per capita:	€ 4.29
Per report:	€ 1.235

Key Organizations:
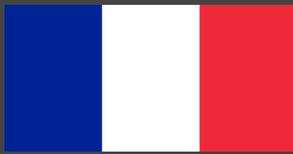
Cybercrime has increased by 10 – 20% annually in France

12,000 French consumers were scammed by seven websites selling face masks and hand gel which never arrived

The **Gendarmerie Nationale Cyberspace Command** (COMCYBERGEND) has been fully operational since August 2021 and has brought together all the Gendarmerie's specialized units. It has 11 local branches, and it coordinates a network of 7,000 specialized officers from local correspondents who are trained to carry out simple cybercrime investigations, to departmental, regional and national expert investigators. This new organization aims at streamlining the cybercrime fighting activities.

COMCYBERGEND works closely together with the public-private partnership **ACYMA (Actions Against Cybermalveillance)** launched in 2017. Its mission is to increase awareness, prevent cybercrime and provide aid to both consumers and companies.

Consumers can report cybercrime both to the Police via **Internet Signalement** as well as on the website of the ACYMA, often the first point of reference for cybercrime victims. The reports are added to the PHAROS, Platform for Harmonization, Analysis, Cross-checking and Orientation of Reports, system.

The Ministry of Economy and Finance also offers a portal to report fraud, **SignalConso.** All reports are stored in the Fraud Repression Database (DGCCRF). Law enforcement may decide to investigate if a report warrants this. From September 2020 to August 2021 92,346 complaints were received, more than half of which were related to online services.

According to the ACYMA the Covid-19 pandemic resulted in an increase in cybercrime. Phishing in all its forms remains the most common crime followed by account hacking. The third place in the ranking is occupied by fake tech support scams, closely followed by ransomware which grew significantly increased in 2020.

Chart — Share of Respondents

Legend: ■ During the past 6 months ■ During the past 12 months

Category	During the past 6 months	During the past 12 months
Pishing	20%	11%
Scam or embezzlement	9%	7%
Bank fraud	6%	8%
Someone has impersonated abother person	5%	8%
Ransomeware (ransom for unlock)	5%	7%
Stolen identity on the internet	5%	7%
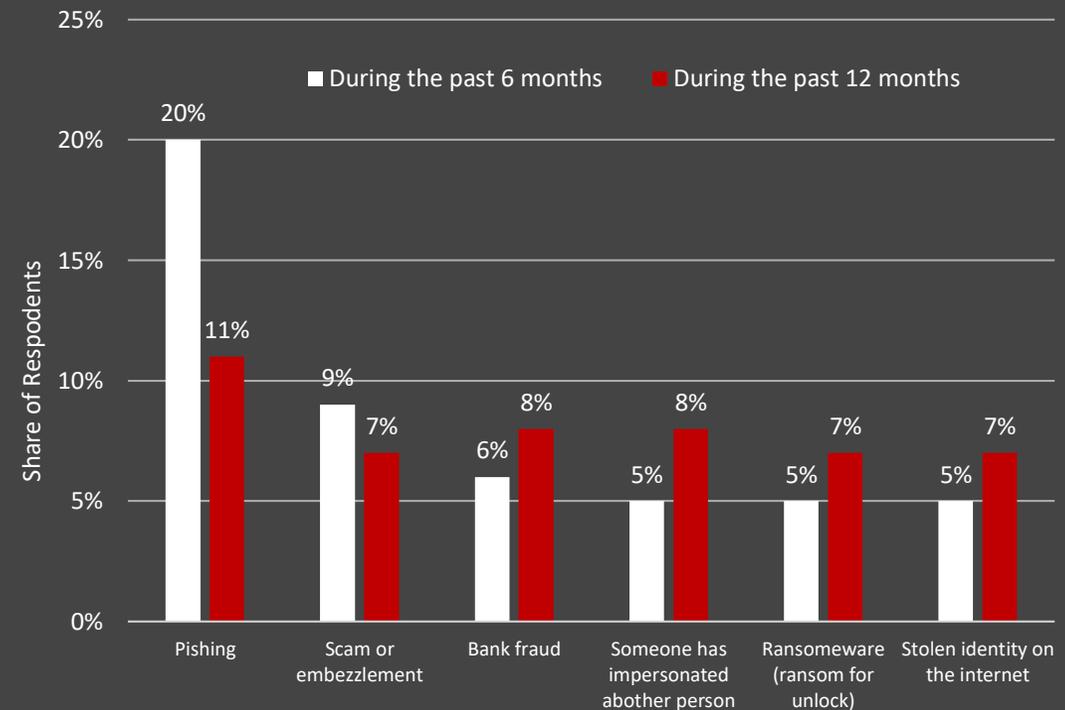
Key Statistics:

Population:	67 million
Internet:	90%
# of Scams:	46,173 (15%)
Scams / 1,000 :	0.7
Money lost:	€ 162 million*
Per capita:	€ 2.40
Per report:	€ 3,500

Key Organizations:

POLICE NATIONALE — internet-signalement.gouv.fr — Cyber Malveillance.gouv.fr (Assistance et prévention en sécurité numérique) — Com CyberGend — Signal Conso

***** ScamAdviser Expert Estimate**

In 2020, the number of scams increased by 9% in Germany

Scam fighting is fragmented across the sixteen German states

According to the German Constitution, police jurisdiction lies with the federal states. Germans can report online crimes to the police authority of their state. Most states offer an **Internet Wache** (Internet Watch) service. In addition, consumers can also turn to the **Verbraucherszentrale**, the consumer protection centers. The Verbraucherzentrale are likewise mainly organized at the state level with some of them supporting online reporting.

The **Bundeskriminalamt (BKA)** is part of the Federal Ministry of Internal Affairs. Its main goal is to coordinate crime suppression at the national and international level. Within the BKA the Serious and Organized Crime (SO) subdivision Cybercrime (SO-4) conducts investigations, coordinates national and international activities, and analyzes current cybercrime phenomena. The focus of the unit is more on malware, extortion software, and DDOS attacks and less on consumer related fraud. The BKA - SO4 also coordinates the **Zentrale Ansprechstelle Cybercrime** (ZAC), the central point of contact for cybercrime. Each state has its own ZAC.

The **German Federal Office for Information Security** also advises and counsels consumers on digital risks and recommendations.

The joint police forces offer a website to prevent crime called **Polizei Beratung**. Cyber related crimes is one of the topics tackled. The website also provides general statistics on cybercrime. In 2020 320,323 internet related crimes were reported, a 9% increase compared to 2019. 59% of the reported cases were solved. Of the 124,557 criminals identified 70% were male.

Verbraucherschutz.com is a popular private initiative that allows consumers to report scams and warns consumers about new kinds of scams.

polizei-beratung.de/presse/infografiken/

Reported internet violations 2020

- Other crimes; 23%
- IP violations; 1,30%
- Adult content; 5%
- Credit fraud; 2,80%
- Performance fraud; 1,60%
- Computer fraud; 3,30%
- Other Fraud; 11,20%
- Credit card fraud; 18,90%
- Merchandise Fraud; 32,60%
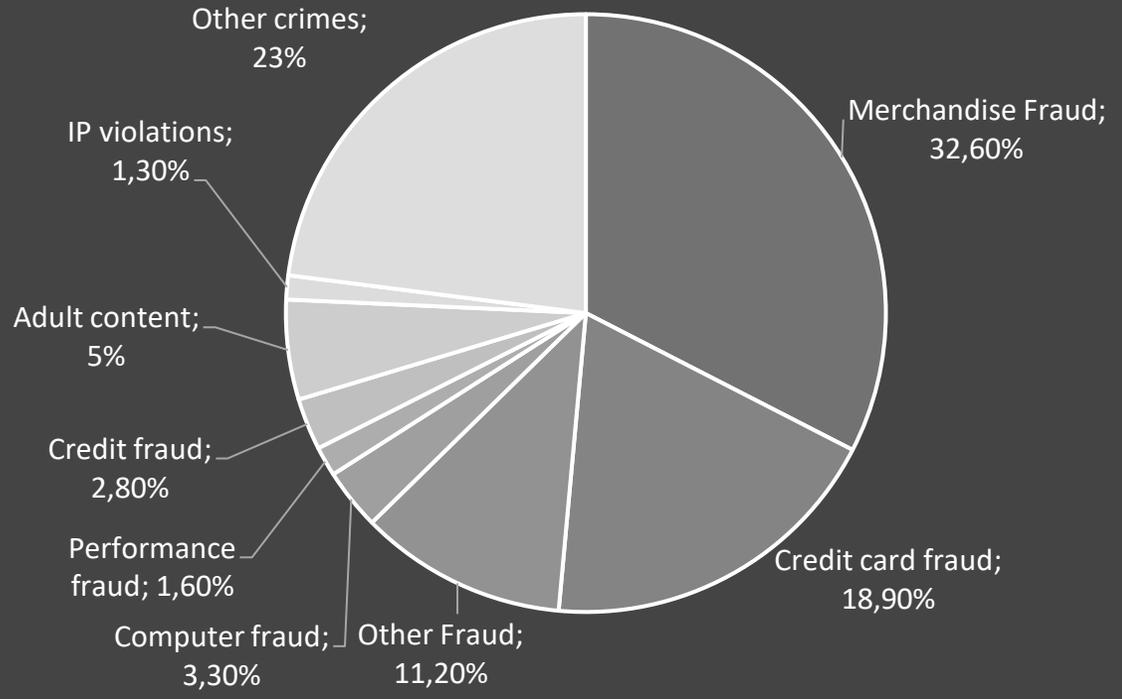
Key Statistics:

Population:	83 million
Internet:	95%
# of Scams:	320.232 (9%)
Scams / 1,000 :	3.8
Money lost:	€ 3.1 billion
Per capita:	€ 37,14
Per report:	€ 9,696

Key Organizations:

- Bundeskriminalamt - SO-4
- Zentralen Anspechstellen Cybercrime
- Verbraucherschutz.com

India has been hit hard by scammers due to Covid-19

Fraudsters used the pandemic to scam victims with fake mask, oxygen, hospital beds and drugs

The **Ministry of Electronics and Information Technology** supports the overall development of IT, digitalizing and dealing with matters relating to Cyber Laws.

The **Serious Fraud Investigation Office** is a multi-disciplinary organization under the Ministry of Corporate Affairs, consisting of experts in the field of accountancy, forensic auditing, law, information technology, investigation, company law, capital market and taxation. It focuses on detecting and prosecuting or recommending for prosecution white-collar crimes and frauds.

The **National Cybercrime Reporting Portal** is an initiative of the Ministry of Home Affairs launched to facilitate victims/complainants to report cybercrime complaints. At present, this portal caters to complaints pertaining to online Child Pornography/ Child Sexual Abuse Material or sexually explicit content such as Rape/Gang Rape content. Other cases can be reported to the local police by dialing 100.

In 2020, India was hit hard by cybercrime, experiencing close to **120 million cases**. Overall, cybercrime increased by 86% between the months of March and April 2020 alone. In the period from August 2019 to June 2021 Rs 79.68 crore was lost to cyber frauds.

From fake medicines to fire extinguishers disguised as oxygen cylinders and recycled personal protective equipment, India's Coronavirus hell has been lucrative for its ever-inventive army of scammers, with sometimes deadly consequences.

The percent of suspected fraudulent digital transaction attempts against businesses increased by 28.32%.

The rapid adoption of digital payments and internet availability in India has resulted in a large growth in the number of scams and money lost. However, 52% of adults do not know to protect themselves against Cybercrime.

The most common scams are:
- Credit Card/Banking Phishing Scams
- Fake Government sites & emails
- Documents Cloud Phishing Scams
- Fake Jobs
- Lottery Scams
- Fake Government body emails
- Event Phishing – like sporting events, concerts

WhatsApp (89.6%) is the most used messenger tool for scams, followed by Telegram (5.6%) and Viber (4.7%).

Key Statistics:

Population:	1,380 million
Internet:	41%
# of Scams:	120 mil. (85%)
Scams / 1,000 :	87
Money lost:	€ 21 billion
Per capita:	€ 15.42
Per report:	€ 177.29

Key Organizations:

Ministry of Electronics and Information Technology

National Cyber Crime Reporting Portal

Serious Fraud Investigation Office

techwireasia.com/2021/07/cybercrime-is-rising-and-apac-users-can-do-more-to-fight-it/
thehindu.com/sci-tech/technology/over-29-lakh-cyber-security-incidents-related-to-digital-banking-reported-in-2020/article33757241.ece

In two years, online fraud increased by 200% in Iran

However, the number of bank scams could be reduced by 90% through the enforcement of multi-factor authentication

The **Cyber Police of the Islamic Republic of Iran** was established in 2011 in order to prevent, investigate and combat cybercrime. It is part of the **FATA police force** of Iran.

The **Cyber Police** has several duties. It monitors and coordinates actions to protect the religious and national identity or Iran. It also takes preventive and active measures to ensure that the values and norms of Iranian society are enforced. In addition, the police unit fights cybercrime, including foreign attacks on its Information infrastructure. Thirdly, it focuses on protecting consumers from online (credit) fraud, phishing and privacy breaches.

Consumers can report digital crimes both through **cyberpolice.ir** (only accessible from an IP address within Iran) which is maintained by the Cyber Police unit, as well as on the general website of FATA police.

There is a separate court to handle cybercrimes. Cyberfraud can be punished by up to 3 years in prison and confiscation of property.

The most common types of scams are bank account phishing and non-delivery of ordered goods. With the introduction of multi-factor authentication, bank card phishing has been reduced by 90% in a few months time. The remaining 10% of bank card phishing scams are due to people not having enabled this feature on their cards and to malware, able to steal dynamic passwords.

Popular scam platforms are Facenama (comparable with Facebook), Telegram and Instagram. Facebook and Google are blocked in Iran. With the rise of online scams and cybercrime, the Ministry of Internal affairs is considering legalizing and organizing the Internet more efficiently as well as launching a national information network.

Key Statistics:

Population:	84 million
Internet:	80%
# of Scams:	(100%)
Scams / 1,000 :	-
Money lost:	-
Per capita:	-
Per report:	-

Kev Organizations:

FATA Police

Cyber Police

In Ireland online Fraud increased with 43% in 2020

The amount of money lost increased with 5%

The **Garda Síochána** facilitates the online reporting of crimes for amounts less than €1000. Citizens can also visit a local police station or call a specific number. In general, the Garda Síochána encourages victims to personally report crime.

The majority of online fraud in Ireland is investigated by either local Police Units or the **Garda National Economic Crime Bureau** (GNECB), which focuses on the more complicated, international and organized crime cases. The GNECB provides support and expertise to local investigators and trains 50 new Detectives each year in fraud-investigation, in conjunction with University College Dublin (UCD). Staff is seconded to Office of the Director of Corporate Enforcement (ODCE), the Department of Social Protection (DSP), and the Office of the Competition and Consumer Protection Commission (CCPC). The GNECB also operates Ireland Financial Intelligence Unit (FIU).

The **Garda National Cyber Crime Bureau** is the national Garda unit tasked with digital forensic examination and investigations into digital criminal offences. Where the GCECB takes on larger cases of online fraud, the GNCCB, which was reinstated in 2017, focuses on cybercrimes like DDOS attacks and ransomware.

The cyber crime team has investigated 324 'phishing' incidents and 178 'business email compromise' cases between February and October of 2020. In this period, there were also 149 'investment frauds' and 43 incidents of 'unauthorized access' to computer systems. Finally, reported romance fraud increased by 37%.

In the first half of 2021 39,9 million was lost in fraud, an increase of 5% compared to the previous year. Most money was lost through acts of deception (€ 9 million), investment fraud (€ 8 million), account take-over (€ 5 million), and BEC (€ 3,5 million).

The Central Statistics Office records combined online and offline fraud. Overall, fraud reported to the police dropped by 1.4% to 7,818, a small drop compared to that witnessed in other types of crimes. For example, burglary and related offences were down by 5,810, or 34.7%, and robbery, extortion and hijacking offences were down by 536, or 22.9%.

FraudSMART is a fraud awareness initiative developed by the Banking & Payments Federation Ireland (BPFI). The Initiative aims to raise consumer and business awareness of the latest financial fraud activity and trends.

Key Statistics:		Key Organizations:
Population:	5 million	
Internet:	89%	
# of Scams:	7,818 (+43%)	
Scams / 1,000 :	2	
Money lost:	€ 75,81 million	
Per capita:	€ 15,18	
Per report:	€ 9,696.-	

We focus on catching the 'king pin' behind a scam

Interview with Michael Cryan, Detective Superintendent and 2nd in Command Garda National Economic Crime Bureau

Can you describe the "Fraud Situation" in Ireland?

The development of online scams in Ireland follow the same trend as the rest of the world. Personal data is being stolen in large scale attacks and in more personalized attacks via text, call, and email. Websites of brands are being cloned to sell fake products.

We also have seen a significant rise in consumers seeking investments after being approached by intermediaries that are not registered and regulated by our Central Bank. Fraud related to Card Not Present increased by 500% in the first half of 2021. Likewise phishing/vishing/smishing fraud reports increased by 440%. Investment fraud increased by 120% and Romance Scams are up 105%.

During the Covid-19 pandemic Romance fraud increased as people could not meet and socialize and covid restrictions was the great excuse for the fraudster not being able to meet. Welfare fraud also increased with fraudulent claims of Pandemic Unemployment Payments being made. Covid restrictions helped to reduce some types of frauds as there was less movement of people, shops and business closed. For example, employment/internal fraud decreased by 42%.

How does the Garda National Economic Crime Bureau combat online scams?

We try to build more public awareness. Nearly every week we publish a case, both in national papers and in the local media. Each case highlights a recently exposed scam. In this way the public is made aware of the workings of different kinds of scams.

In terms of enforcement, we are focussing more on catching the "king pin" behind the fraud. Money mules are a big issue in Ireland as without them Organized Crime and Gangs (OCGs) would have difficulties cashing out the proceeds of their frauds.

Michael Cryan
Detective Superintendent and 2nd in Command
Garda National Economic Crime Bureau

Israel is the most targeted country by cybercriminals

In 2020 Israel made it into to the top of the list for cybercrime plagued countries with 180,000 identified hacking attempts.

Cybercrime in Israel is mostly dealt with by four main units. Israel **Police National Cyber Crime Unit** (Lahav 433) investigates criminal offences. The unit is staffed by 50 police officers and an additional 25 national service youths and IDF soldiers. In addition to the police's main cyber unit, each district has its own cybercrime squad that investigates simpler cases.

The **National Cyber Bureau** at the Prime Minister's Office is responsible for all aspects of cyber defense in the civilian sphere, from formulating policy and building technological power to operational defense in cyberspace. Part of the bureau is Israel's CERT team for Cyber incident handling.

The **Cybercrime Department in the Israeli State Attorney's Office**, set-up in 2015, prosecutes cyber offences.

Finally, the Israeli **Privacy Protection Agency** investigates database-related offences.

Israeli citizens can report online crimes to all kinds of organizations. Remarkably, online scams can also be reported to Israel's CERT team via the 119 hotline.

The Israeli Police handled 8,377 cases of cyberattacks against Israeli targets over the course of 2020. **The most common complaints include identity theft (2,093) and digital forgery (2,795).** Interestingly, although one of the most common cybercrimes worldwide is the theft of credit cards and other forms of electronic payment, in Israel only 350 such cases were opened in 2020.

Only 9% of victims of cyber crimes in Israel report them to the police. The police therefore launched a campaign urging the public to turn to them regarding incidents of online fraud and theft by sending phishing emails to a special email address.

5 צעדים פשוטים שיסייעו לכם להיערך ולהפחית סיכוי למתקפת כופרה

הקפידו על עדכוני תוכנה | התקינו תוכנות הגנה בסיסיות | בצעו גיבויים

מתקפת כופרה- **זה העסק שלך!** מומלץ להיעזר באנשי מקצוע בתחום | הכינו תוכנית מגירה | גלו עירנות להודעות דיוג ומתחזים

סייבר ישראל מערך הסייבר הלאומי | לדרכי התגוננות ולדיווח על אירועי סייבר **119**

Key Statistics:

Population:	9.2 million
Internet:	76%
# of Scams:	8,377 (50%)
Scams / 1,000 :	0.9
Money lost:	-
Per capita:	-
Per report:	-

Key Organizations:

State Attorney – Cyber Unit

National Cyber Center

Italy was the European country impacted the most by Covid-scams

In March 2020 the Italian police arrested the first 36 people who offered, but not delivered, masks or herbal "cures"

The Post and Communication Police was set-up in 1981 to protect the privacy and freedom of any form of communication of Italian citizens. In 1996, its charter was extended towards the IT domain. Nowadays, the Post and Communication Police consists of 2,000 police officers who specialize in IT. It is spread across 20 regional offices. The organization focuses on several areas including child pornography, cyberterrorism (managed by a special unit called CNAIPIC), copyright infringement, hacking, protection of the national communication infrastructure, e-banking and online gaming and betting.

The State Police has largely delegated online crime to the Post and Communication Police. The State Police does, however, support campaigns to warn Italian citizens about online fraud.

Within the Post and Communication Police a special **Cyber Crime Analysis Unit** has been set up in close cooperation with Italian Universities to study computer crimes.

On the website of the Post and Communication Police consumers can find information about online fraud and report online crime. Online crime reports are passed along to one of the 20 regional police offices.

Altroconsumo is the largest independent consumer organization in Italy and counts on the support of 700,000 consumers. The organization supports its members with online shopping issues through its "Easy Claim" service.

Between August 2020 and July 2021 155,242 fraud cases were reported. 50% of these were cybercrime related. This reflects a growth of 16% (physical crimes dropped by 67% in the same period). Apart from Covid-19 specific scams, the police also reported an increase in investment and online trading scams and romantic dating fraud.

Total number of frauds in Italy from August 2017 to July 2021

Period	Number
August 2017 to July 2018	122378
August 2018 to July 2019	134535
August 2019 to July 2020	133633
August 2020 to July 2021*	155242
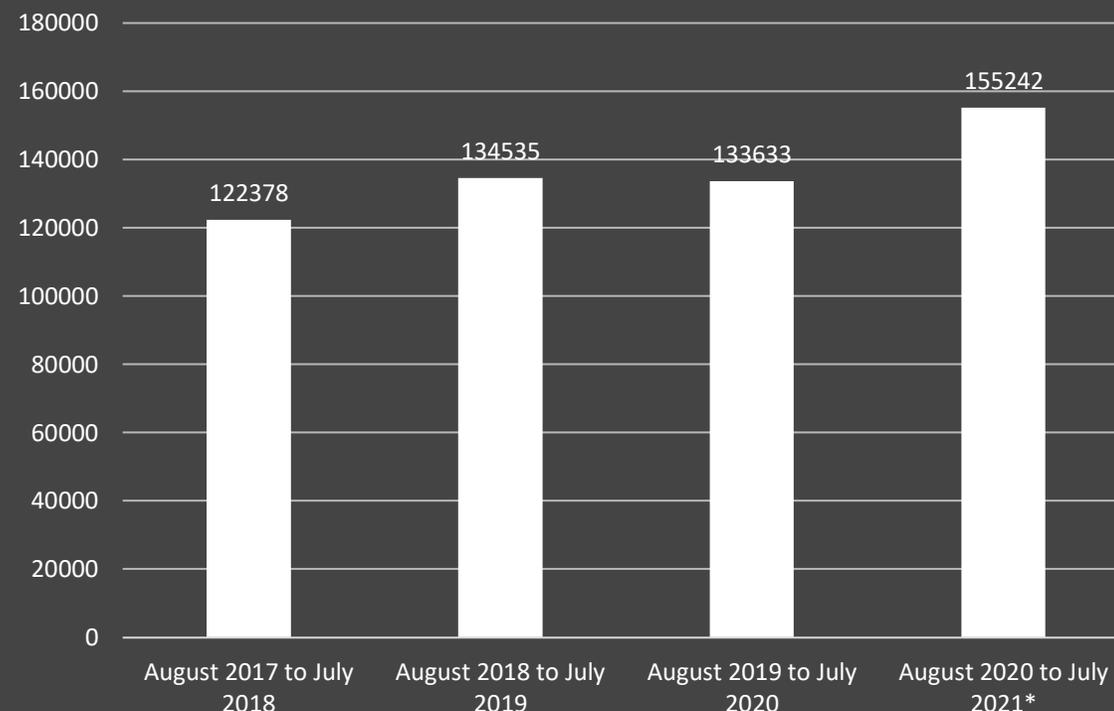
Key Statistics:

Population:	59,6 million
Internet:	92%
# of Scams:	77,621 (+16%)
Scams / 1,000 :	1.3
Money lost:	€ 156.6 million*
Per capita:	€ 2.63
Per report:	€ 2,017

Key Organizations:

polizia delle comunicazioni

ALTROCONSUMO

* ScamAdviser Expert Estimate

In 2020, Japan's online fraud dropped by 5%

However, the number of malicious webshops reported increased by 30% from 7,764 in 2019 to 10,095 in 2020

In Japan, 'Fraud' offence is generally defined in Article 246 of the Penal Code. Japan currently does not collect data on online scams although it collects data on fraud, which includes phone calls where elderly people are tricked to transfer money.

@Police is a website operated by the High-Tech Crime Technology Division of the National Police Agency, whose purpose is to prevent cyber crimes and cyber attacks. Although the website provides information, consumers cannot report scams directly.

Instead, they are encouraged to report scams to the local police station. In addition, several private organizations have also set up websites to receive public victim reports.

The **Safer Internet Association** (SIA) gathers data about malicious e-commerce website from consumers. The data is shared with the **Japan Cybercrime Control Center** (JC3) for further analysis and action.

JC3 is a public-private partnership organization that works closely with industry, universities and law enforcement to address cyberspace threats. Established in 2014, JC3 focusses on threat collection, developing countermeasures and training.

The number of fraud offenses reported to the Police in Japan was 30,468 in 2020, (compared to 32,207 in 2019). The amount of money lost dropped by 12% to 27.8 billion Yen. In the first half of 2021, the Safer Internet Association reported 6,535 malicious online stores, an increase of 30% compared. Malicious sites increasingly imitate shopping sites for cooking utensils and appliances. Likewise, the number of crypto investment scam sites nearly tripled in the last year. Scam sites are mainly found via search engines (65%), email (13%) and messengers apps (7%). The most common payment methods used were bank transfers (60%), and credit card (20.5%).
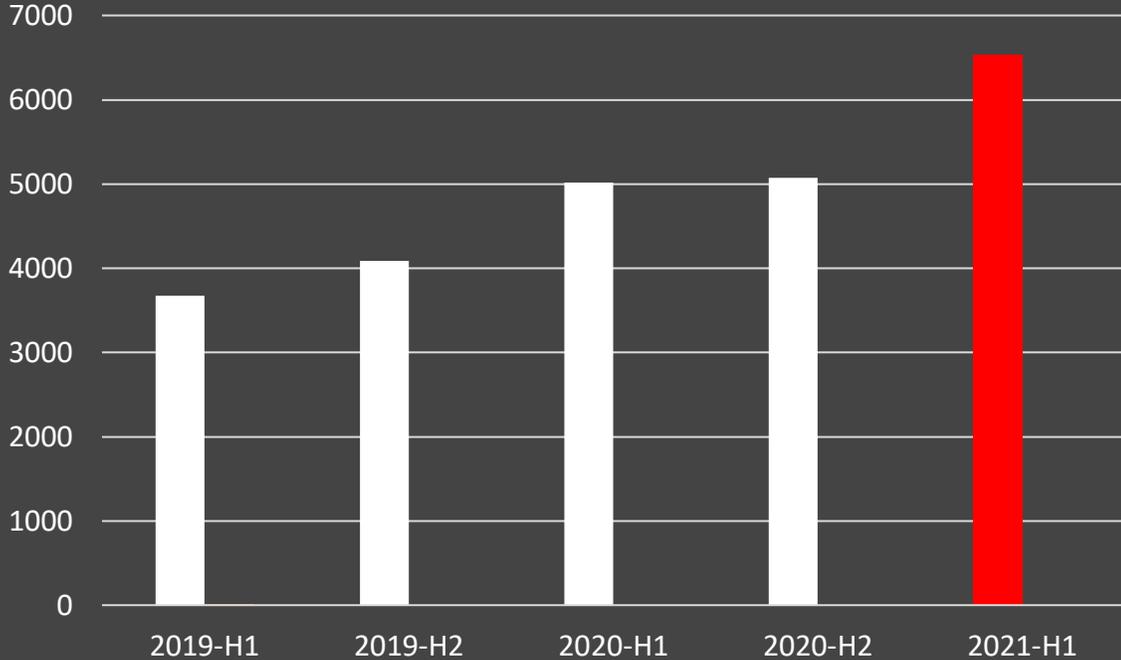
Number of reports of malicious shopping sites

Key Statistics:
Population:	126 million
Internet:	94%
# of Scams:	40,581 (-5%)
Scams / 1,000 :	0,4
Money lost:	€ 217 million
Per capita:	€ 1,72
Per report:	€ 5,343

Key Organizations:

JC3 日本サイバー犯罪対策センター
JC3: Japan Cybercrime Control Center

SIA 一般社団法人セーファーインターネット協会
Safer Internet Association

Japanese can earn 10,000 Yen by scamming the scammer

The Japanese Police is strengthening the fight against scam in any way possible

The "ore ore scam" is one of the oldest cons in Japan. Senior citizen are called, and the scammer says, "Ore da," or "It's me." The idea is that the victim will think the scammer for a family member, and asks "Who is this?" the scammer will respond with "What? It's me! You recognize my voice, don't you?". Scammers play the "son" or "grandson".

The scammer will subsequently tell the victim that money is needed, quickly! To pay off a debt, a mistake made at work, etcetera. Of course, the "son" or "grandson" can't pick the money up in person and says a friend or coworker will do so, or that the money must be transferred to a co-worker's account.

The Minami Precinct launched Operation *Pretend to Be Fooled*. This new crime-fighting program asks people who have been contacted by someone claiming to be a family member or friend in need of cash to notify the police. The potential victim and police then work together to catch the scammer. The targeted victim later receives 10,000 yen (€ 77.50).

Statistics on what are referred to as "special frauds" show that the total number of "ore ore scams", saving scams involving the impersonation of police officers or staff at financial institutions in order to obtain card details to withdraw money from bank accounts fell by 5.1% from 2019 to 2020, in which 6,382 cases were reported. Instead, the financial losses resulting from such scams rose by 3.4% to 12.2 billion yen. Thus, even though the total number of cases fell, financial losses increased by around 400 yen between 2019 and 2020.
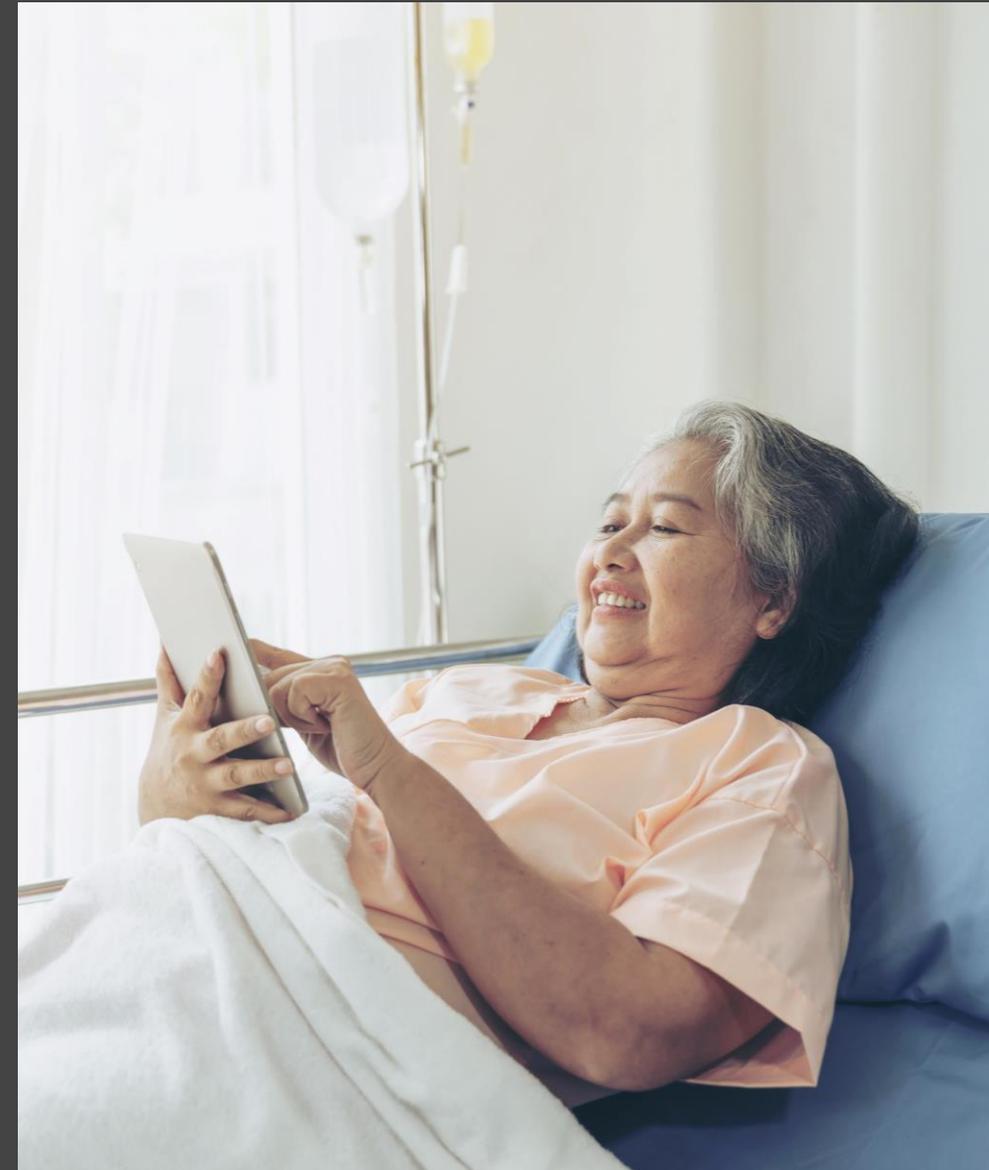
Online fraud is not yet a high priority in Kenya

The Kenyan government faces other issues such as combating corporate as well as government corruption and consumer fraud

Online scams can be reported to the **Kenya local and national Police**. Action from the police is usually slow and inconsistent. The process of reporting must be done physically rather than digitally. As a result, few consumers report scams.

The principal aim of the **Digital Forensic Laboratory** (DFL) is to identify, seize, acquire and analyze all electronic devices related to cyber-enabled offences reported in order to collect digital evidence which can be presented in a court of law. The DFL is part of the Directorate of Criminal Investigations which falls under the National Police Service. The CERT team is part of the DFL. Consumers can report incidents to the DFL via phone and email.

There is little data available on cybercrime in Kenya. According to Abacus, $148 million was lost through cybercrime in Kenya in 2015. Serianu, a cybersecurity company, reported a loss of $295 million in 2019.

Overall, it appears that that the number of online scams is increasing rapidly. Most Kenyans are not tech savvy enough to browse the internet carefully, spot fake ads and sites by verifying technical details or checking reviews.

A growing number of fake online stores advertise heavily on social media. Scammers show superior products but deliver poor quality goods or do not deliver at all. The Amazon Web Worker app scam, a kind of Ponzi scheme, made the news. Many Kenyans fell for the scam as they trusted the Google App Store and Amazon's brand name. Phone scams, especially those involving mobile payment platforms such as MPESA and Airtel Money increased sharply as well. Most phone frauds are 'relative in distress' scams, followed by 'false money reversal request' scams.

DCI KENYA @DCI_Kenya

A suspect believed to have obtained millions of shillings from Kenyans in a fraudulent scheme known as Amazon Web Worker, was arrested yesterday after she jetted into the country, from the U.S.

Invest 3600Ksh, You can earn 210Ksh DAILY. Monthly 6,300 ksh

Invest 8000Ksh, You can earn 535Ksh DAILY. Monthly 16,050 ksh.

Invest 20,000Ksh, You can earn 1350KSH DAILY. Monthly 40,500 Ksh.

Invest 50,000Ksh, You can earn 3400Ksh DAILY. Monthly 102,000 Ksh.

Key Statistics:

Population:	53.7 million
Internet:	87
# of Scams:	-
Scams / 1,000 :	-
Money lost:	251.6 million
Per capita:	€ 4,68
Per report:	-

Key Organizations:

Digital Forensic Laboratory

* ScamAdviser Expert Estimate

Malaysia reported an increase of 33% in online scams

In June, 45% of all complaints received by the Ministry of Domestic Trade and Consumer Affairs were related to scams

Scams have been on the increase since the COVID-19 pandemic hit Malaysia. The Malaysian government enforced lockdowns or Movement Control Orders (MCO) which are largely still in place in 2021. Consumers rely on shopping online for their needs and many cybercriminals are taking advantage of this situation to scam vulnerable consumers who fail to realize that they are not purchasing from registered platforms.

Consumers can report online scams both to the local police, the Central bank of Malaysia, and the **Commercial Crime Investigation Department (CCID) Scam Response Centre**. The CCID Scam Response Center was set up in March 2021 as a one-stop report and response center, especially for Macau scams.

Believed to have originated from Macau or that the first victims came from there, Macau scams often start with the victim being approached by someone pretending to be an officer from a bank, government or law enforcement agency or debt collector. The scammer will claim that the potential victim owes money or has an an unpaid fine, often with a very short window of less than an hour to settle the payment or face the consequences. In 2020, 6,003 Macau cases were reported (compared to 725 in 2019) , with RM287,301 million being lost (compared to RM254,586 in 2019).

To combat Macau scams, the CCID launched the Semak Mule site for the public to verify accounts that could potentially be used by scammers.

Shopping online via social media has become more popular as people are looking for products which are cheaper than the price offered by registered platforms. The most common forms of scams, together with non-delivery, are bitcoin mining, Macau scams, and love scams. As shopping is moving to social media, most scams are now also carried out via Facebook and Instagram.

FOMCA, the Federation of Malaysian Consumer Associations, has been asking the government to take aggressive steps in tracking down scammers and to demand that sellers register with the government agencies.

CCID, Facebook Malaysia, in partnership with FOMCA launched a nationwide #TakNakScam awareness campaign to educate consumers on how to identify, check and report scams.

#TakNakScam
SPOT   CHECK   REPORT

Key Statistics:

Population:	32.4 million
Internet:	81%
# of Scams:	11,511 (33%)
Scams / 1,000 :	0.4
Money lost:	€ 56.8 million
Per capita:	€ 1,76
Per report:	€ 4934

Key Organizations:

CCID Scam Response Center

Federation of Malaysian Consumer Associations

70% of all fraud-related crime in Mexico is now digital

In June, 45% of all complaints received by the Ministry of Domestic Trade and Consumer Affairs were related to scams

The **National Guard (Guardia Nacional)** has a division for scientific investigation that also receives reports of fraudulent activities, scams, extortion and other malicious activities. The National Guard's helpdesk number, 088, was set up to receive reports from consumers. The Government of Mexico created the **Cyber Prevention and Investigation Unit** (formerly Policía Cibernética) as part of the Guardia Nacional.

There is a unified model for cyber police operations (modelo homologado de policía cibernética) adopted by each state police department that also have a cybercrime team focused on online scams, cyberbullying and phishing.

PROFECO is the national authority for consumer protection. The organization collects reports of fraudulent activities and processes them for further investigation. Although they offer a help desk service, the organization is not focused on online scams but on products and services that do not match their description. However, PROFECO maintains a list of complaints against online stores as well as a blacklist of malicious ones.

CONDUSEF is part of the national government and monitors the financial service providers in Mexico. It also creates educational material and provides financial information for transparency purposes for Mexican citizens to make informed decisions about the benefits, costs and risks of financial services being offered. Like PROFECO, they maintain a white and blacklist of service providers and track online fraud reports and resolutions from financial institutions. CONDUSEF has been gathering data on online fraud for several years, reporting 1,378,689 cases in the first trimester of 2021, as well as 3,180 million pesos lost (€135 million).

The **Mexican Internet Association** (AIMX) focuses on raising both consumer and company awareness concerning cybersecurity, as well as pleading for better legislation.

Source: Mexican Internet Association (AIMX), CONDUSEF

Traditional Fraud vs Online Fraud

Legend: ■ Traditional ■ Cyber
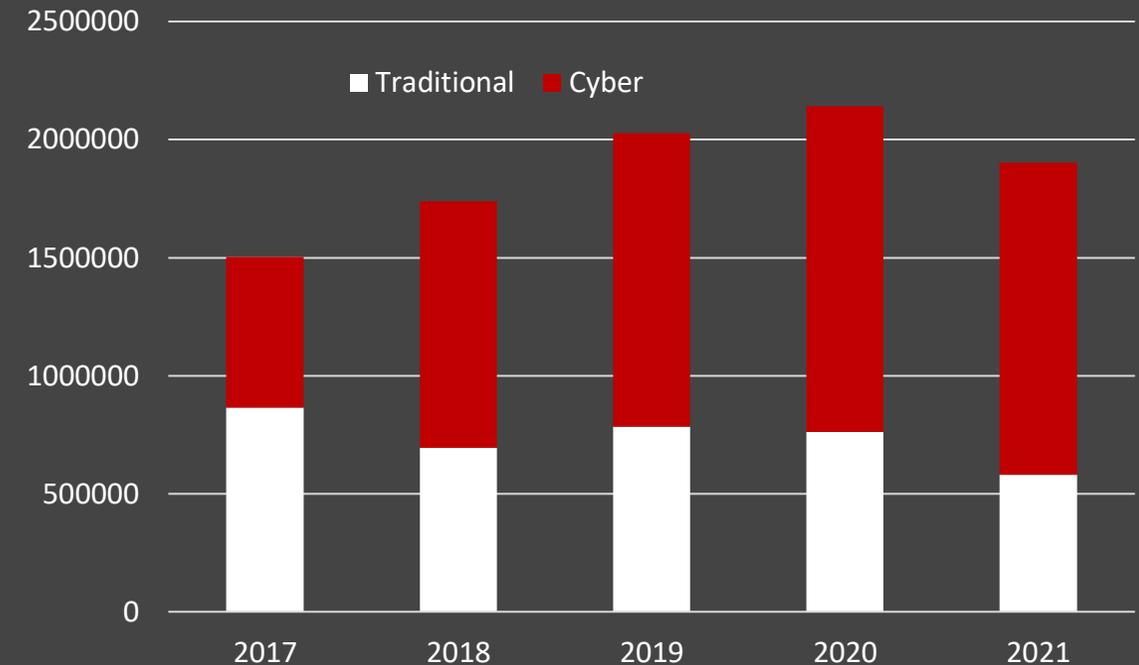
Key Statistics:

Population:	129 million
Internet:	69%
# of Scams:	5.5 million (11%)
Scams / 1,000 :	43
Money lost:	€ 386 million
Per capita:	€ 2,99
Per report:	€ 70

Key Organizations:

GUARDIA NACIONAL · JUSTICIA Y PAZ

PROFECO · PROCURADURÍA FEDERAL DEL CONSUMIDOR

CONDUSEF

Asociación de Internet MX.

Mass media reach is needed to educate the public in Mexico

Pablo Corona Fraga, Deputy VP of Cybersecurity, Mexican Internet Association (AIMX)

How would you describe the cybercrime situation in Mexico?

As the number of cybercrime incidents increases in Mexico, so does the attention of the government and companies toward such crimes. However, there is much room for improvement. In 2020, an estimated 25% of Mexican companies were attacked by cybercriminals. This number is staggering!

In 2020, the Mexican e-commerce market grew by 30%. The number of online scams grew accordingly. Online scams are by far the biggest issue of the Internet in Mexico right now.

What does the Mexican Internet Association do to make the internet safer for Mexicans?

We launched a program called *Safe Internet for Everyone*. We have developed guides helping companies boost their cybersecurity and developed an educational program for schools. We also launched a social media campaign to educate consumers called **#LikeIntelligente**. The campaign was set up to increase cybersecurity awareness through memes and short messages. The campaign has been very well received and it even won a price from the OECD as one of the best South American projects.

AIMX also published its first cybersecurity report and will continue to do so for the coming years. Additionally, we are expanding our cooperation with the digital investigation unit of the National Guard to build awareness.

How can we win the war against online scams?

You cannot fight cybercrime as a whole. The biggest challenge is a lack of budget to use mass-media. The best way to reach Mexican consumers continues to be via TV and radio and we would love to increase the reach of our #LikeIntelligence campaign.

On the policy side, AIMX is working on improving and expanding legislation, improving cybercrime related statistics and expanding our network of partners to combine efforts.

Pablo Corona Fraga
Deputy VP of Cybersecurity
Mexican Internet Association (AIMX)

Scams in the Netherlands grew by 50% due to easier reporting

The number of WhatsApp phishing scams saw an especially significant growth . Most money was lost in investment/cryptocurrency schemes

There are several organizations working together in the Netherlands to combat online fraud. The most important ones are **FraudeHelpdesk**, a public private-partnership (PPP) which helps consumers to find the right support, and the **Dutch Police Online Crime Report Center** which aggregates all online crime reports coming in and coordinates these across the 10 regional police units.

ECP is a PPP which stimulates cooperation to create a safe and prosperous Dutch digital community. It does so amongst others, including **VeiligInternetten.nl**, a website offering tips and tricks to consumers on how to use the Internet safely and **AlertOnline** which helps build cybersecurity awareness amongst Dutch companies.

Other organizations involved in building cybersecurity awareness and in reporting of online fraud are the **Authority Financial Markets** (AFM), **Authority Consumer Markets** (ACM) and the **Dutch Payment Association** which also has an informational site called **SafeBanking**. The Dutch Payment Association reported €26,7 million in losses.

Fraudehelpdesk reported a growth of 57% in losses, from €26 million in 2019 to €41 million in 2020. The PPP received 350.000 emails, mostly about phishing and malware. In addition, it received 120,000 calls concerning a.o. identity theft, fake family and friends help request via WhatsApp and online buying and selling scams. The foundation states that scammers are becoming more professional, first gathering public data on the victim to personalize the approach, e.g., using names of friends/family. Most money was lost in investment/cryptofraud; on average, €32,000, followed by advanced fee scams and BEC.

The Dutch Police received 120,696 reports of fraud. 61% of reports were filed digitally. The increase was caused both by Covid-19 as well as by making online reporting easier. At the moment only 13% of Dutch victims report being scammed.

Sources: Fraudehelpdesk, Dutch Police

Money Lost per Scam Type (€)

Legend: — Phishing   — Card Not Present

Y-axis: 0, 2000000, 4000000, 6000000, 8000000, 10000000, 12000000, 14000000
X-axis: 2016, 2017, 2018, 2019, 2020
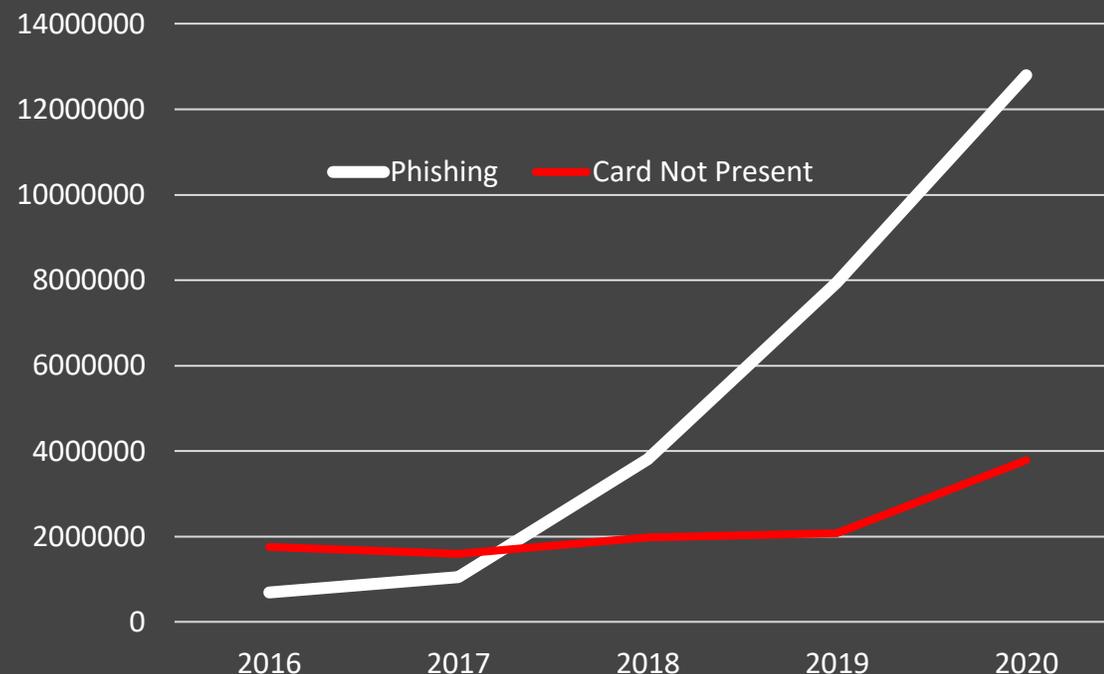
Key Statistics:

Population:	17.4 million
Internet:	94%
# of Scams:	120,696 (50%)
Scams / 1,000 :	6.9
Money lost:	€ 80,5 million
Per capita:	€ 4,62
Per report:	€ 1.076

Key Organizations:

POLITIE

FRAUDEHELPDESK.nl

consumentenbond

ECP

Fraudsters are becoming increasingly professional

Interview with Tanya Wijngaarde, Communication & Press Officer at Fraudehelpdesk

We continue to see reports of online fraud increase, despite all the warnings.

Fraudsters are constantly looking for new opportunities, especially digital ones. For example, we see that fraudsters manage to obtain growing amounts of information before they make their move.

For example, they first steal your bank account login details via a phishing link and then call you posing as a bank employee who indeed knows everything about your recent transactions.

In other cases, they already have complete data profiles at their disposal thanks to a data leak. This allows them to target specific groups, for example people over 50.

With all that personal information, cybercriminals come across as reliable and convincing, and that's why people are more likely to fall for their scams.

Tanya Wijngaarde
Communication & Press Officer
Fraudehelpdesk

In New Zealand, scams rose by 69%

The largest single loss reported was approximately NZ$ 840,000 (€506,000)

Citizens in New Zealand can report scams to several organizations. Cybercrimes can be reported to the **New Zealand Police** online. The police also offers information and links to relevant organizations concerning cybercrime in general as well as online fraud.

The **Financial Market Authority** also offers online reporting and maintains a list of names of businesses or individuals one should be wary of when planning to invest.

CERT NZ also offers companies and consumers the option to report cybercrime including scams both online and via phone. CERT NZ received 3,410 phishing and credential harvesting reports, up by 76% compared to 2019; it also received 1,920 scams and fraud reports, up by 11% compared to 2019. NZ$ 16.9 million (€11.5 million) was reported lost.

All organizations also revert to **Netsafe**. Netsafe was founded in 1998 as non-profit organization to help New Zealand internet users stay safe online. Netsafe provides free and confidential advice and support to people in New Zealand seven days a week. Each week it responds to about 450 requests for help related to online safety including bullying, grooming, illegal content and scams via email, online and by phone. The organization is financially supported by the Ministries of Education and Justice as well as by an additional 350 members. It works together with the Commerce Commission, Department of Internal Affairs, Financial Markets Authority, Ministry of Consumer Affairs, National Cyber Security Centre and the Police amongst others.

NetSafe received 14,790 scam reports in 2020. In 3,954 cases money was lost, totaling NZ$ 19 million (€11.5 million). The largest single loss was NZ$ 840,000 (€506,000). As scams are reported to multiple other organizations and many do not report scams out of shame, NetSafe considers the statistics to be only the tip of the iceberg.

Category	Number of reports	Total Loss (NZ$)	Average Loss (NZ$)
Investment fraud	367	7,053,577.47	19,377.96
Relationship and trust fraud (romance scams)	252	4,721,250.53	18,735.12
Products and services fraud	2,509	3,309,104.36	1,318.89
Prize and grant fraud	280	1,121,599.54	4,005.71
Phantom debt collection fraud	32	696,390.01	21,762.19

Key Statistics:
Population: 5.1 million
Internet: 86%
# of Scams: 14,790 (69%)
Scams / 1,000 : 4.0
Money lost: € 21.7 million
Per capita: € 4,26
Per report: € 1,076

Key Organizations:

Education is not enough; we have to share information globally

Interview with Sean Lyons, CTO of NetSafe New Zealand

Can you describe how scams are developing in New Zealand?

I have seen a year-on-year increase since I have been working for Netsafe (ed: 15 years). The amount lost also continues to increase. This keeps surprising us as the population of New Zealand is becoming more Internet-savvy and educated. Despite the fact that they are increasingly equipped to recognize scams and tend to report them more, the amount of money being lost keeps increasing.

This increase may be caused by the fact that scams are always changing and are also increasing in sophistication. New scams pop-up with every new disaster and new technology. This even occurs with disasters you would not expect to provoke a rise in scams, such as the Evergreen containership blocking the Suez channel. In that instance, within 24 hours we received the first phishing emails with the Evergreen as theme. No global event is free from being misused by scammers.

What does Netsafe do to protect consumers?

Any citizen of New Zealand can contact us for support regarding child grooming, cyberbullying, scams, etc. In many cases we offer victim support anonymously. Sometimes we refer to the right channel such ad law enforcement while in other cases we mediate. We also work together with platforms to prevent cybercrime. In addition, we run programs to educate children, students and employees, to build resilience. One of our most important tips is that one should use consumer friendly payment methods.

How can we fight scams on a global level in a more efficient way?

I thought the answer was in education. However, scams are getting better and better. The inconvenient truth is that scammers will always be able to find the right victim at the right moment. Anybody is vulnerable at some point in their life. We have to share information early to warn consumers about new scams faster. If a scam pops up in Europe, 24 hours later it is in New Zealand and vice-versa. Sharing data is the only way forward. Some of this data will be privacy sensitive and require changes in the law.

Sean Lyons
Chief Technology Officer
NetSafe New Zealand

COVID-19 hit Nigeria hard, as scams grew by 186%

In particular, young people fell for scams in a desperate attempt to make a livelihood

Where consumers can report a scam depends on the type of scam in question. Victims can report to the (local) police or go to the **Nigerian Police Cybercrime** Reporting Portal. If the scam is financial in nature the crime can be reported to the **Economic and Financial Crimes Commission** (EFCC).

The Nigerian Inter-Bank Settlement Service (NIBSS) reported that fraudulent activities were detected 46,126 times between January and September of 2020, an increase of 186% compared to 2019. Out of these attempts, 91% were successful. In the same period, Nigerian financial service companies recorded losses amounting to 5.2 billion Naira, a 510% increase from the 550 million Naira recorded in 2019. 65% of the losses occurred between July and September 2020. Social engineering has remained the most potent tool of choice, as it was seen to be responsible for 56% of fraud attacks in 2020.

There is little to no enforcement of cyber laws as stipulated in the 2015 Cyber Crime Prohibition and Prevention Act. This is worsened by the fact that most of the punishments stipulated in the Act tend to not match the crimes committed.

Scams below the threshold of 20,000 Naira (€41) are likely to go unreported. The stress and cost of obtaining a police report and court affidavit to initiate a complaint with the bank discourages most victims as they feel the effort needed to go through such a process is not worth it.

Another problem has been that of Ponzi schemes. While regulators such as the Securities and Exchange Commission have tried to clamp down on such schemes, their proliferation continues to rise.

The **CyberSafe Foundation** is a Nigerian NGO that facilitates a safer internet space for everyone with digital access in Nigeria. Boosting scam awareness and exposing online fraud is one of their main focus areas.

"While Government agencies, regulatory bodies, and law enforcement continue their valiant efforts in fighting fraud and cybercrime, lack of synergistic cooperation, paucity of data, and adequate enforcement of regulations continue to hamper their efforts. As Scam and fraud actors continue to improve their methods there is an urgent need for a cross collaborative strategy between government and private sector to fight the menace of fraud and cybercrime in the country."

CyberSafe Foundation

Key Statistics:

Population:	206 million
Internet:	61%
# of Scams:	61,500 (186%)
Scams / 1,000 :	0.3
Money lost:	€ 10,7 million
Per capita:	€ 0,05
Per report:	€ 175

Key Organizations:

During lockdown, scams increased sharply in Pakistan

The number of Internet users grew by 35% in 2020

Citizens can report scams and other cybercrimes online at the **Federal Investigation Agency** (FIA). Complaints are then passed along to the **National Response Centre for Cyber Crime** (NR3C), also called the Cybercrime Wing. The NR3C was set-up in 2007, as part of FIA, and it is the law enforcement agency in Pakistan dedicated to fighting cyber crime. Scams are also reported to the **Pakistan Telecommunications Authority**, to telecom operators, and to banks.

Cyber Security of Pakistan is the flagship program of CS Zone and builds awareness and knowledge for a cyber secure Pakistan. It also set up Cyber Scouts as the new legislation forces companies to educate their employees about cyber threats and cyber hygiene. Cyber Scouts are students who promote awareness about cyber crime in the society. A Cyber Scout is selected and trained to identify cyber crime activities and equipped with adequate preventive knowledge to help fight the menace. Last year, the organization also set up The Stress Counseling Desk to support cybercrime victims.

NR3C handled around 94,764 complaints of online crimes, including financial fraud, sexual harassment, cyber stalking, and access to unauthorized accounts last year. As a result of the complaints, 621 parties accused from 22 different groups were arrested and more than 20,000 electronic devices were confiscated by the agency.

The amount lost in scams is unknown. However, in one investment scam alone more than 100,000 Pakistani lost over RS 5.6 billion (€28 million).

Data from the advocacy organization **Digital Rights Foundation** (DRF) shows that during the lockdown period, Pakistan witnessed a sharp rise in the number of cybercrime cases. The DRF registered 3,246 complaints via their helpline and social media in 2020.

The DRF's data states that 68% of the complainants were made by women and their cases ranged from fake profiles to data theft, cyberbullying, blackmailing, etc. The FIA reports that 70 to 80% of complaints they received were filed by women.

Crime Category	2018	2019	2020
Financial Frauds	2358	11905	30318
Harassment	1112	5120	16023
Hockino	1171	5837	7966
Delamation	713	3641	6004
Fake Profile	5005	7140	4456
Un-authorized Access	1339	3957	3905
Blockmailing	450	2381	3447
Threats	537	2027	2756
Misc.	136	335	1674
Online Shopping	264	1284	1471
Sialking	393	981	1304
Blasphemous Contents	133	1126	711
Identify Theft	114	780	573
Anti-Relcion	68	641	543
Online Job Frouds	187	778	514
Spoofing	109	242	463
Lottery Frauds	99	289	275
Online Banking Frouds	65	341	206
Spammino	40	226	184
Pornography	27	161	173
Illegal SIMs	15	144	121
Anti-Govt.	47	256	92
Child Pornography	1	19	83
Phishing	4	105	40
Digital Currency	5	67	20
Total	**14392**	**49783**	**83322**

Key Statistics:

Population:	220 million
Internet:	32%
# of Scams:	94,764 (97%)
Scams / 1,000 :	0.9
Money lost:	28 million
Per capita:	€ 0,26
Per report:	€ 297

Key Organizations:
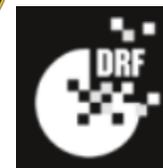
Our biggest issue in Pakistan is a lack of cybercrime awareness

Interview with Muhammad Asad Ul Rehman, CEO of CSZone

How would you describe the cybersecurity situation in Pakistan?

80% of the crime is caused by a lack of cybercrime awareness. People do not use safe passwords and are very vulnerable to social engineering aiming to steal their money (unclear?). The most popular kind of scam is financial fraud. Some scams are very simple. People are called and are offered a "call girl" for a very low price. They pay and the call girl never arrives. Of course, the victim does not go to the police.

What does Cyber Security Pakistan do to combat online fraud?

Cyber Security Pakistan is a team of ethical hackers, cyber security experts, researchers and cyber scouts whose primary purpose is to build a cyber secure community by promoting awareness of cyber security in Pakistan. Furthermore, it includes HR training and capacity building to address the real-world challenges of cyber security.

Our Cyber Scout initiative is very successful. We trained more than 700 people, both citizens and law enforcement officers. For 2021 we expect a sharp increase in this number.

In addition to cyber capacity building at universities, schools and companies, we offer stress counseling via social media and phone. The service is especially used by girls who have been victims of cybercrime. Finally, we regularly publish cybercrime alerts via social media to warn consumers, companies and government entities about new forms of scams.

How can the government of Pakistan fight against Cyber crimes?

In 2016, the Prevention of Electronic Crime Act, know as PECA16, was implemented. As the hackers tried to hack the Prime Minister's account last month, government attention to cybercrime has increased sharply and the government of Pakistan announced a new Cyber Security Policy. The Cybercrime Wing is picking up speed and growing rapidly. More cybercriminals are being apprehended. The reporting process can still be improved as the website where citizens can report scams often does not work. Most citizens prefer to report scams physically but there are only 15 reporting centers in Pakistan. Finally, the legal process has to become more efficient in order to allow law enforcement to focus on apprehending cybercriminals.

Muhammad Asad Ul Rehman
CEO CSZone

The police of the Philippines reported a 37% increase in scams

The number of Cybercrimes in general decreased by 4.26%

Several organizations are responsible for fighting cybercrime in the Philippines; among these is the Department of Justice Office of Cybercrime (OOC). The OOC is the central authority in all matters relating to international mutual assistance and extradition for cybercrime and cyber-related matters. It also acts as the focal agency in formulating and implementing law enforcement investigation and prosecution strategies in curbing cybercrime and cyber-related offenses nationwide.

The **Cybercrime Investigation and Coordinating Center** (CICC), which was set-up in 2012, is an agency linked to the Department of Information and Communications Technology (DICT). The CICC is responsible for the formulation of the National Cybersecurity Plan, the National Computer Emergency Response Team (CERT), and the facilitation of international intelligence cooperation, especially regarding cybersecurity matters that are transferred to the Department.

The Philippines' **National Police Anti-Cybercrime Group** (PNP-ACG) focuses on cyber forensics, investigations and arrests. The organization has 21 Regional Anti-Cybercrime Units across the country.

The ACG reported that 869 online scams were recorded from March to September 2020, an increase of 37.28% compared to the 633 incidents occurred in the same period the previous year. Identify theft where people are posing as other persons to commit crimes increased by 21.47%, from 298 to 362.

The ACG noted that during quarantine cybercrimes decreased by 4.26%, from 3,001 to 2,873. Among the notable decreases are voyeurism, which fell from 390 to 255 or 34.61%, computer hacking, which fell by 50.52% from 190 to 94, illegal access (159 to 127, or 20.12%) and online libel (711 to 683, or 3.93%).

Key Statistics:

Population:	110 million
Internet:	72%
# of Scams:	1,738 (37%)
Scams / 1,000 :	-
Money lost:	-
Per capita:	-
Per report:	-

Key Organizations:

REPUBLIC OF THE PHILIPPINES
CYBERCRIME INVESTIGATION AND COORDINATING CENTER

In the Philippines, the pandemic has brought out the worst in people

Interview with Nathaniel Rabonza, Chief Intelligence Processing Division, Philippines Cybercrime Investigation and Coordinating Center

How would you describe the internal cybersecurity situation in the Philippines?

The government of the Philippines seems to be a favorite target of hacking, given the number of defaced websites in recent years. The Cybercrime Prevention Act of 2012 controversy alone attracted numerous cyberattacks from subgroups allegedly attached to Anonymous Philippines. With high hopes, the Department of Information and Communication Technology (DICT) has developed a cybersecurity plan to set up by 2022. The DICT acknowledges its mandate to "ensure the rights of individuals to privacy and confidentiality of their personal information; ensure the security of critical ICT infrastructures including information assets of the government, individuals and businesses; and provide oversight over agencies governing and regulating the ICT sector and ensure consumer protection and welfare, data privacy and security, foster competition and the growth of the ICT sector." They said that one of their priorities is to ensure that the country is cyber secure from the national to the individual level. According to the National Cybersecurity Plan 2022, they aim to achieve a nation "assuring the continuous operation of our nation's critical infostructures, public and military networks, implementing cyber resilience measures to enhance our ability to respond to threats before, during and after attacks, effective coordination with law enforcement agencies and a cybersecurity educated society."

To what extent are online scams an issue in the Philippines?

In the Philippines, the pandemic has brought out the worst in some opportunists, and in the virtual realm, it appears phishing attacks are the cyber weapon of choice. The Philippines has been trying to enforce legislation on phishing scams for years, but with so many Filipinos online all the time during the pandemic, the National Bureau of Investigation's Cybercrime Division recorded a 200% increase since the lockdown started back in March.

Phishing is being listed by the authorities as the top cybercrime being committed, followed by online selling scams, and the spread of fake news.

A worrying trend that cybersecurity observers in the Philippines have noticed is that some of the larger organizations and individuals might not be reporting incidents of their personal data being breached, owing to stigma in the country that could view a loss of such critical data as an indicator of disrepute. Hence, the phishing and cybercrime rates might be even higher than previously reported, and Filipino cybersecurity practitioners state that many businesses are not aware of the full extent of the threats against them.

What actions have been taken in the last year by your organization?

The Cybercrime Investigation and Coordinating Center (CICC) was established in August 2020. The CICC is one of the agencies linked to the DICT for policy and program coordination. The CICC is exploring the use of current and emerging technologies in the fight against cybercrime. Cybercrime has become the fastest growing socio-economic crime. The government aims to shield and safeguard the Philippines "from computer generated attacks that could cause massive crises in our economy, banking and financial institutions, communications and other critical infrastructure". Lately, the agency also conducted cybercrime operations against illegal sex dens/establishments in various areas in NCR and South Luzon..

How can we make sure consumers are scammed less?

Governments must promote programs to develop the cybersecurity awareness of the people as well as establish and maintain internal controls specifically designed to prevent and detect fraud. If unsure of the legitimacy of a business, one should take to do a bit more research to ensure that the process is safe; never share any personal information, especially social security or tax ID numbers, account numbers, or login and password information via email or text. When needing to communicate sensitive information with your bank via email, be sure to use a secure email within the bank's secure online banking platform. Do not share passwords and do not leave any documents that contain access to financial data in an unsecured area. Change your passwords regularly for better protection, using a combination of letters, numbers and special characters when possible. Change your wireless network default password as well as the default SSID (name used to identify your network). Don't broadcast your SSID and consider using encryption on your network. Emails are designed to prompt you to click on links provided within the email to verify or change your account in some way. Often, the links included in the email are ways for fraudsters to install malicious software onto the computer or device you use to access your email. With cyber-attacks on the rise, it's more important than ever to install antivirus software on your computer or network. Equally important is ensuring you are regularly running and updating this software to prevent viruses from infecting your computer. Keep your computer operating system and Internet browser current; this provides additional protection against fraud and theft.

Poland reports a rise of 116% in phishing attacks

The government is committed to expanding the cyberteam within the police to 1,800 officers by the year 2025

NASK (Research and Academic Computer Network) is the registry of the .pl TLD and its key tasks also include that of ensuring Poland's internet security. Early on, it set up a Computer Incident Response Team (CSIRT) where users could report incidents.

In August 2018, **CERT Polska** was entrusted with the role of CSIRT NASK as defined by the National Cybersecurity System Bill. The CERT Polska team operates within the structures of NASK. It provides a consumer help desk where it is possible to report an incident (incydent.cert.pl).

In addition, NASK offers a contact point for reporting illegal content (dyzurnet.pl) especially related to the sexual abuse of children. NASK also set up **saferinternet.pl** which is part of the **Polish Safer Internet Center** (PCPSI). The PSICSI has been working for over 15 years to increase public awareness of online threats, combat illegal content online and provide psychological help to children, parents and professionals in the event of threats related to the use of new technologies.

The police offers citizens the option to report cybercrime online. In 2020 The Polish government began investing significantly in the cybercrime team of the police. The goal is to have 1,800 officers working for the cyber police by 2025.

CERT Polska reported 3,516 phishing scams in 2019. This number grew to 7,622 cases in 2020. The organization started a new initiative to report "bad domains" online and make the list available in several technical formats to the public to warn them. its main recipients are the ISPs. CERT Polska/CSIRT NASK) has signed an agreement with the largest ISPs, the Minister of Digital Affairs and the Office of Electronic Communications so that the phishing sites are blocked automatically at an ISP level. The list is also used by various browsers (Opera, Google), smaller ISPs, phishing AdBlock lists and so on.

https://www.24newshd.tv/27-Jul-2021/poland-creates-cyberpolice
https://cert.pl/uploads/docs/Raport_CP_2020.pdf

Incidents received by CERT PL
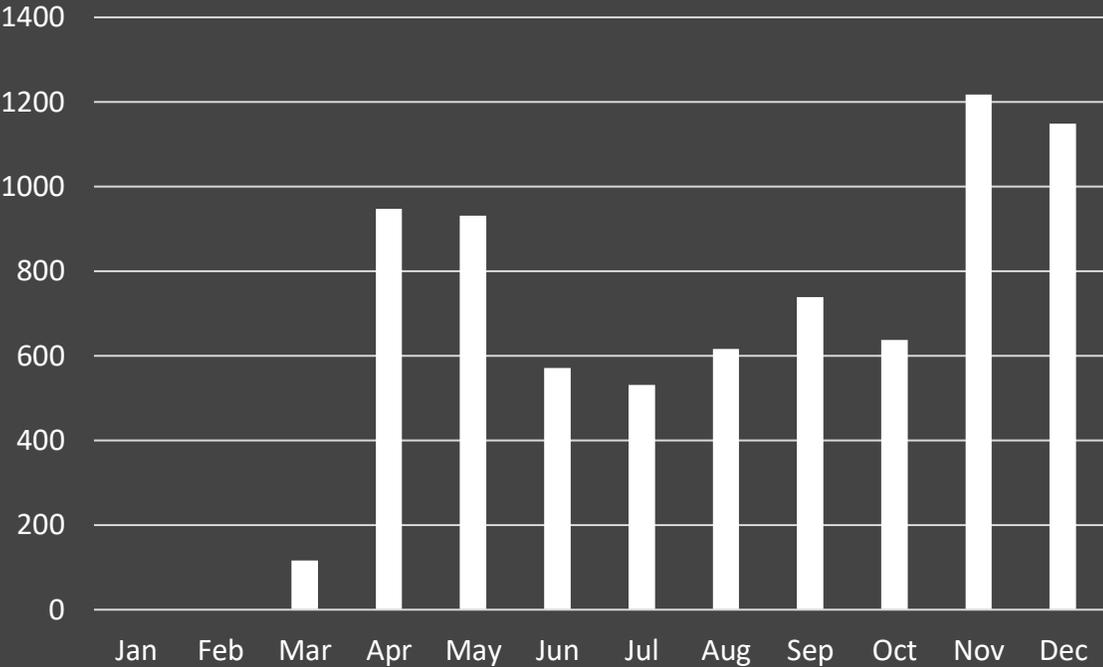
Key Statistics:

Population:	38 million
Internet:	78%
# of Scams:	7,622 (116%)
Scams / 1,000 :	0.1
Money lost:	3.8 million*
Per capita:	€ 0.37
Per report:	€ 1.080

Key Organizations:

NASK   POLICJA

saferinternet.pl

NASK CERT.PL

* ScamAdviser Expert Estimate

In 2020, online fraud in Portugal increased by 22%

Government agencies and the police have started paying more attention to online fraud

The **Portuguese National Cybersecurity Centre** (CNCS) mission is to contribute to a free, reliable and safe use of the Internet in Portugal. It acts as the operational coordinator and national authority on cybersecurity between state departments, national critical infrastructure operators, essential and digital service providers.

The key focus areas of the CNCS are cybersecurity awareness building and training for a safer and more responsible use of the Internet. This includes the production and dissemination of warnings, guidelines, and good practices for the safer use of technology by citizens and organizations. It also involves monitoring and advising about the state of national cybersecurity through its **CERT.PT** service, which coordinates the response to incidents that affect the cyberspace of national interest.

In 2016 the Criminal Police (Polícia Judiciária), formed the **National Unit to Combat Cybercrime and Technological Crime** (UNC3T). Its main competencies are prevention, detection, criminal investigation and assistance of judicial authorities regarding crimes committed by computerized means.

Portuguese citizens can report scams online on the websites of the Polícia Judiciária, of the Public Prosecution Service and its Cybercrime Office, and of CNCS.

Several organizations are also building awareness around scams. The CNCS informs the public and supports in the recovery from cyberincidents. **Deco Proteste** is the largest consumer protection organization in Portugal and offers an online complaint forum. 81% of the complaints were closed in the last year. The organization offers both information on scams online and support via phone.

CERT PT, as part of CNCS, identified 1,347 cybersecurity incidents in 2020. This reflects an increase of 79% compared to the year before.

By sector, attacks on banking more than tripled in 2020, reaching 229 incidents and making this sector the second most attacked. The most relevant scams registered in Portuguese cyberspace during 2020 were phishing, smishing, sextortion and fraud using a mobile payment application.

Incidents received by CERT PT
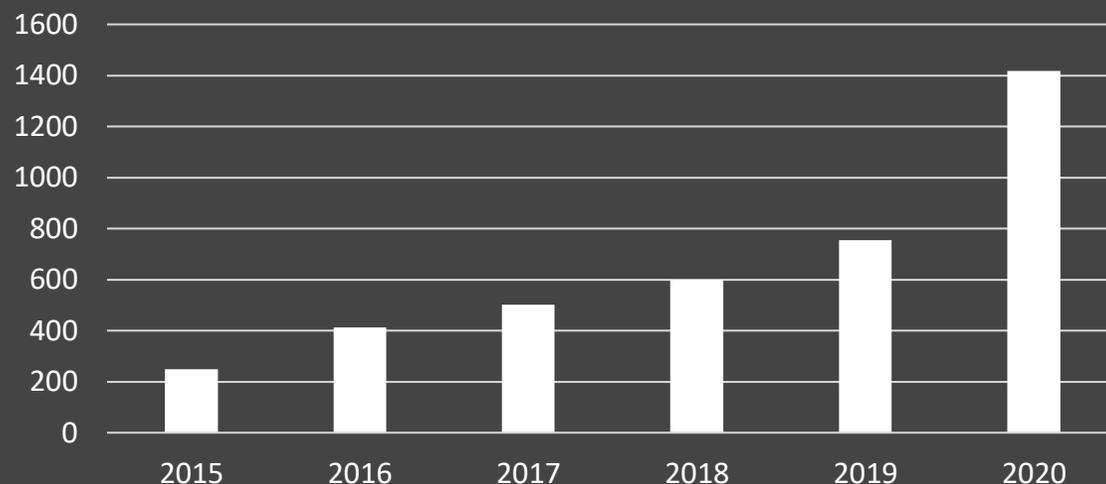
Key Statistics:

Population:	38 million
Internet:	78%
# of Scams:	1,347 (22%)
Scams / 1,000 :	0.1
Money lost:	1.3 million*
Per capita:	€ 0.07
Per report:	€ 991

Key Organizations:

CNCS, 2021: cncs.gov.pt/docs/relatorio-riscosconflitos2021-observatoriociberseguranca-cncs.pdf
cibercrime.ministeriopublico.pt/sites/default/files/documentos/pdf/relatorio_riscos_conflitos2021.pdf

* ScamAdviser Expert Estimate

Russian scammers moved to robocalls to reduce costs

In this way, they were able to steal over 150 billion rubles (€1.74 billion) in 2020

Russians can report online fraud to several organizations including the Russian **Consumer Protection Agency**, the **Health Inspection Service** (for drugs), the **prosecutor's office** and the police. The police recently also set up a special CyberSecurity team.

To combat financial scams **Financial CERT has been set-up by the Bank of Russia as a** Computer Emergency Response Team. Financial CERT facilitates information exchange between financial market participants, law enforcement agencies, telecom providers and operators, system integrators, anti-virus software developers, and other companies engaged in information security activities.

ROCIT is a public organization uniting active Internet users in Russia. One of its services is a hotline where Russians can report fraud, low quality Internet services, unscrupulous online stores, hacked accounts, etc.

In 2020, telephone and online fraudsters earned about 150 billion rubles from Russians; of these, 66 billion rubles were stolen by scammers pretending to be bank employees; 46.5 billion were stolen via fictitious medical services; 18.6 billion were stolen through phishing and fake online stores.

Health related scams proved the most financially rewarding for scammers. 930,000 Russians lost an average 50,000 rubles. The number of Russians falling for bank related scams is larger, 4.4 million but on average they "only" lost 15,000 rubles.

Compared to 2019, the number of scams and phishing detected by Group-IB in Russia and CIS grew by 35%. Group-IB detected over 70 scam groups employed in a single fraudulent scheme, Classiscam; 54 of them were targeted to Russian users. In less than a year, Classiscam threat actors alone managed to steal over 700 million rubles.

A 2020 study by Avast estimates that in 2020 42% of all Russians faced phishing, with 27% falling for the scam. Of the Russians who were victims of phishing, a little more than a quarter (27%) said that they had to change their login details, 13% reported that money was stolen, and 11% reported losing personal data.

Fraudsters have improved their tactics and delegated the primary calls to robots in order to reduce the cost of the attack. In the first half of 2020, the Bank of Russia blocked more than 9.7 thousand fraudulent phone numbers, four times more than the same period the previous year.

Of those who suffered financial losses, 43% lost less than €17,50, 20% lost between €17,50 and €80, 11% lost up to €160, and 5% up to €240. 20% lost more than €240.

Of those who reported the crime, 49% did so to the police, 43% to the company who the cybercriminal pretended to be, 26% shared the scam with colleagues, and 16% informed their email provider.

Key Statistics: **Key Organizations:**

Population:	144 million
Internet:	81%
# of Scams:	5.3 million (35%)
Scams / 1,000 :	37
Money lost:	€ 1.74 billion
Per capita:	€ 12.08
Per report:	€ 327

Sources: GroupIB & tadviser.com/index.php/Article:Phishing_(phishing)
www.kommersant.ru/doc/4627498, crimestat.ru/analytics

Classiscam: 10,000 sites, 70 scam groups and 700 billion rubles lost

A deep dive into automated scam as a service designed to steal money and payment data

Group-IB's Computer Emergency Response Team (CERT-GIB) named the scheme "Classiscam" after witnessing it in Russia in summer 2019. Classiscam has been the most widely used fraud scheme in the world during the pandemic. The scheme targets people who use marketplaces and services relating to property rental, hotel bookings, online bank transfers, online retail, ride-sharing, and delivery.

The scheme is simple and straightforward, which makes it popular. After registering new accounts or using the compromised ones on free classifieds websites, scammers post offers that are too good to be true: goods at low prices aimed at various target audiences. Evildoers ask victims to provide their contact information to allegedly arrange a delivery. The scammer then sends the buyer a URL to either a fake courier service website or a scam website mimicking a classified ads site or a marketplace with a payment form, which turns out to be a scam page. As a result, the fraudster obtains payment data or withdraws money through a fake merchant website. Another scenario involves a scammer contacting a legitimate seller under the guise of a customer and sending a fake payment form mimicking a marketplace and obtained via Telegram bot, so that the seller could reportedly receive the money from the scammer.

The scam system was quickly "exported". More than 40 criminal groups targeted consumers in Bulgaria, the Czech Republic, France, Kazakhstan, Kirghizia, Poland, Romania, Ukraine, the United States and Uzbekistan. It is estimated that most criminal groups made more than $6 million in 2020.

In summer 2020 CERT-GIB took down 280 Classiscam phishing pages offering fake courier services, and by December 2020 that number had grown 10-fold and surpassed 3,000 websites. A total of 44 countries have been targeted in this fraud scheme. According to Group-IB DRP, 93 brands overall have been abused as part of Classiscam. In early 2021, more than 12,500 threat actors made money through fake delivery service resources.

Group-IB was able to expose the hierarchy of the scam groups. Admins are responsible for recruiting new members, creating scam sites and providing assistance when the bank blocks a transaction.

Workers communicate with victims and send them the phishing URLs; they also call pretending to be tech support specialists.

The overall number of websites involved in the scheme reached 10,000. The scale of this type of fraud is immense and the scheme only keeps expanding. One Classiscam threat group alone can make up to $114,000 per month.

GROUP IB

Admins (20-30%)

Workers (70-80%)

Callers (5 – 10%)
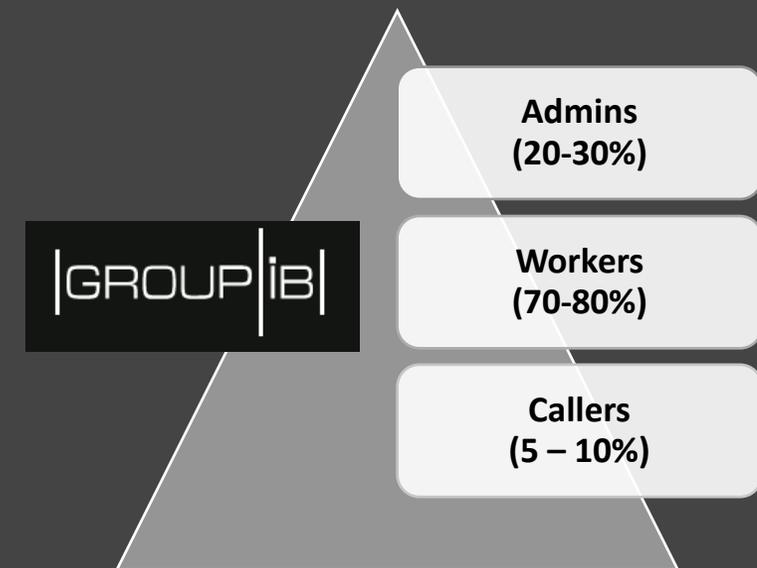
Saudi Arabia has been fighting "big" cybercrime

Increasing attention is directed to cybercrime targeting consumers

Saudi Arabia has been a 'popular' target for cybercriminals for several years as the largest economy of the Middle East, with a high Internet penetration and several political adversaries. In 2020 alone Saudi Arabia recorded over 22,5 million cyber attacks. At the beginning of the Coronavirus pandemic in the first quarter of 2020, the country experienced an increase in malware attacks of 22%, with an increase in spam attacks of 36%.

Several organizations in Saudi Arabia are involved in scam reporting, awareness building and enforcement. The **Saudi Federation for Cyber Security and Programming** (SAFCSP) is the national institution whose goal it is to build national and professional capabilities in the fields of cyber security through awareness, education, and support.

The **Saudi Central Bank** (SAMA) allows consumers to file a complaint related to a financial service including forex and investment scams. The Saudi banks have united to build more cybercrime awareness.

Phone and SMS scam attempts can be reported to the **Communications and Information Technology Commission** (CITC) both online and by phone (330330).

Consumers can report commercial related scams to the **Ministry of Commerce** online, via an app as well as by phone. Other scams from individuals or from outside Saudi Arabia can be reported to the **Ministry of Interior**.

The **Consumer Protection Association** launched a website (scam.sa) in collaboration with the **Ministry of Commerce** to help consumers spot signs of online fraud and learn more about how to protect themselves, with tools to report fraud via text message. The Ministry is also supporter of the "Maroof" ecommerce platform for licensed online stores.

Agencies that the victims contacted.

- Police; 19%
- Saudi CERT; 9%
- Committee for the protection of Virtue and the Prevention of Vice; 10%
- Saudi eGovernment Portal; 29%
- Others(family,friends,selected more than one option from the list); 33%
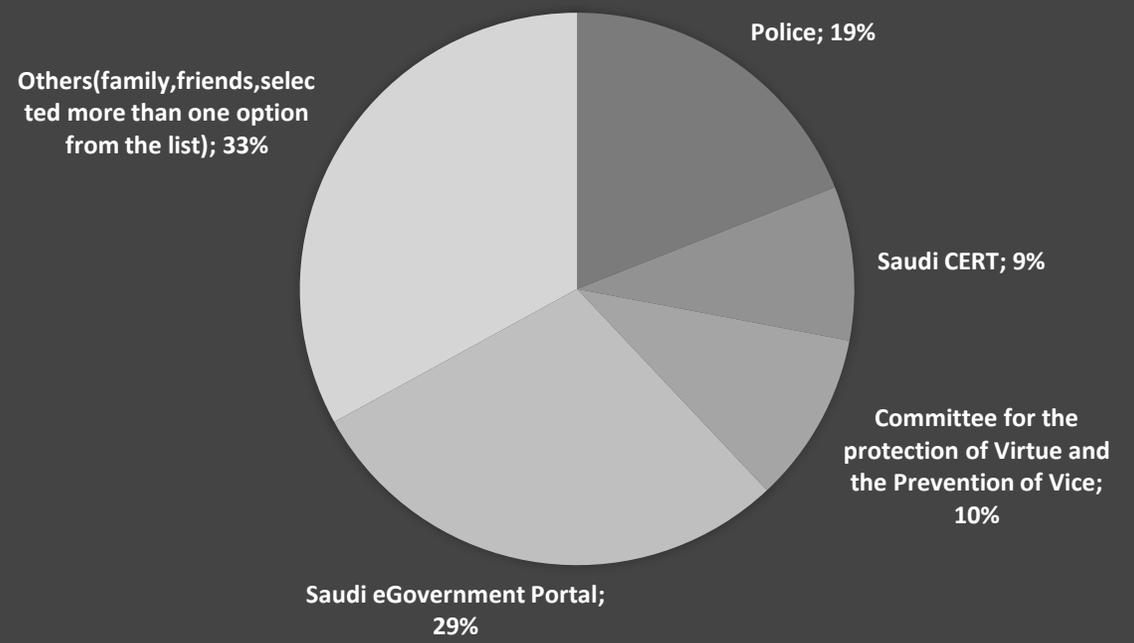
Key Statistics:
Population:	34.8 million
Internet:	92%
# of Scams:	6,595
Scams / 1,000 :	0.2
Money lost:	€ 49.2 million
Per capita:	€ 1.41
Per report:	€ 7,460

Key Organizations:

Scams made up 44% of total crimes in Singapore in H1 2020

The amount of money lost grew by 20%. The trend is expected to continue in 2021

Online Scams have been increasing for several years in Singapore. In 2018 6,189 cases were reported and S$145 million was lost. In 2019 and 2020 9,502 and 14,236 cases were reported (respectively) and S$168 and S$201 million were lost. In the first half of 2021, the number of cases stabilized at 7,400 but the amount grew to S$ 168 in the first half year alone.

To counter this trend the **Singapore Police Force Anti-Scam Centre (ASC)** was set up in 2019. The ASC is the "nerve center" for investigating scam-related crimes and its focus is to disrupt scammers' operations to and help mitigate victims' losses. Its four core activities are Enforcement, Engagement, Engineering and Education. ASC works closely together with more than 20 stakeholders comprising banks, fintech companies, telecommunication companies and online marketplaces in its fight against scams.

The **National Crime Prevention Council** (NCPC) works closely together with the ASC to combat scams. The NCPC, a non-profit organization, is committed to promoting public awareness about crime and to propagate the concept of self-help in crime prevention. The Council comprises representatives from the commercial and industrial sectors, as well as from the public sector and the Singapore Police Force (SPF).

NCPC has launched several initiatives to combat scams. **ScamAlert.sg** offers scam information and has had more than 500,000 visitors in 2020. It also offers a victim support line which handled more than 7,000 calls last year. Apart from lodging reports with the Singapore Police Force, victims are also advised to share their experience on ScamAlert as a form of community effort to combat scams. In 2020, NCPC also launched **ScamShield**, an iPhone app developed in collaboration with Open Government Products to block scam calls and text messages.

Type of scam	Cases reported 2020	Change from 2019	Amount cheated 2020	Change from 2019	Largest sum cheated
E-commerce	3,354	▲ 538	$6.9m	▲ $4.6m	$1.9m
Social media impersonation	3,010	▲ 2,224	$5.5m	▲ $2.4m	$367,000
Loan	1,990	▲ 240	$14.5m	▲ $7.7m	$735,000
Banking-related phishing	1,342	▲ 1,262	$5.8m	▲ $5.3m	$506,000
Investment	1,102	▲ 615	$69.5m	▲ $33.5m	$6.4m
Credit-for-sex	1,023	▼ 43	$2.6m	▼ $200,000	$70,000
Internet love	822	▲ 164	$33.1m	▼ $1.6m	$1.1m
Non-banking-related phishing	644	▲ 595	$981,000	▲ $909,000	$66,000
Tech support	506	▲ 257	$22.3m	▲ $8.3m	$1.1m
Impersonation of China officials	443	▼ 13	$39.6m	▲ $18.5m	$4.2m
Total	**14,236**	▲ **5,839**	**$201.2m***	▲ **$79.4m**	–

Top 10 Scams in Singapore in 2020

Key Statistics:

Population:	5.6 million
Internet:	91%
# of Scams:	14,236 (50%)
Scams / 1,000 :	2,5
Money lost:	€ 127 million
Per capita:	€ 12.08
Per report:	€ 327

Key Organizations:

SINGAPORE POLICE FORCE

NATIONAL CRIME PREVENTION COUNCIL

SCAM ALERT
BRINGING YOU THE LATEST SCAM INFO

Economic & political turmoil in South Africa increases scams with 33%

Governmental resources to fight online scams are still minimal, but commercial organizations are trying to fill the gap

There is no centralized system for reporting cybercrime in South Africa. Citizens can only report scams to their local police office. The **Cybersecurity Hub** is South Africa's National Computer Security Incident Response Team (CSIRT). Incident can be reported online, but since May 2020 no new vulnerabilities have been posted online.

In 2020 the Cybercrime Act was set up, criminalizing cybercrime. It has however not yet been operationalized. Since 2011, the **South African Police Service** (SAPS) has an **Electronic Crime Unit** which focuses mainly on serious crime, solving 80% of the 130 cases in 2020. Under the new law it will have one year to set up a 24/7 cybercrime reporting process. Under the new Cybercrimes Act, provisions of the law will have to be complied with by all affected parties.

To fill the gap, the **Financial Intelligence Centre's** contributes to safeguarding the integrity of the country's financial system. Consumers can check the registration of financial companies on FIC's website as well as report suspicious activities.

The **South African Banking Risk Information Centre** (SABRIC), is a non-profit organization formed by the four major banks to combat organized bank-related crimes. In 2020, SABRIC reported an increase in digital banking fraud of 33% but losses grew by only 0,4%. In total 35,307 digital banking incidents were reported and R309 million was lost. In addition, credit/debit card fraud decreased with 7.2% to R1,067 million.

SAFPS, an NGO, aims to improve vigilance with regards to fraud, financial crime, and identity theft by educating businesses and consumers. It offers a fraud report helpline and maintains a fraud database to assists its members in detecting and preventing fraud and protecting consumers against identify theft and impersonation.

sabric.co.za/media/1388/sabric-annual-crime-stats-2020.pdf
businesstech.co.za/news/business/523168/here-are-the-top-5-digital-scams-in-south-africa-to-be-aware-of/

Most frequent digital fraud schemes targeting consumers

Key Statistics:

Population:	59.3 million
Internet:	55%
# of Scams:	27,928 (33%)
Scams / 1,000 :	0.5
Money lost:	€ 79 million
Per capita:	€ 1.34
Per report:	€ 2,837

Key Organizations:

Cybercrime is under-reported and under-fought in Africa

Interview with Craig Pederson, Director at TCG Digital Forensics

How would you describe the cybercrime situation in South Africa?

In 2020 we have seen a definite increase in both the volume of incidents and in the amount of money lost. Advance-fee scams, dating scams and, of course, Business EMail Compromise (BEC) have risen astronomically. Despite incessant cautions from the banking industry, consumers keep falling prey to these scams.

How is South Africa fighting online cybercrime and scams?

Cybercrime is immensely under-reported in South Africa. All Cybercrime reporting takes place in person at a Police Station. There is a low grasp of technology within ground level policing in South Africa, and many complainants are referred away without the opening of a case. This in turn leads to lower confidence and further under-reporting.

Prosecution rates for cybercrime are equally low. There are a number of Cybercrime investigators nationally that take on pro-bono work through their practices. The law enforcement capacity is immensely hampered. Outdated legislation and very slow transformation of the digital landscape have largely left law enforcement behind. Jurisdictional challenges and slow subpoena processes have added to the complexity of the situation. The overall Cybercrime ability of Law Enforcement on a national basis is nominal when compared to the incidence of crime. Reforms are on the table in the form of a new cybercrimes bill which will take an estimated 3 to 5 years to be fully implemented. As a result, it is not uncommon for scammers to operate with near impunity for 2 to 3 years on the same scam.

What steps should South Africa take in 2021 and beyond?

A paradigm shift needs to take place away from "let's buy software" to "let's invest in skills" in order to adequately address cybercrime. South Africa also needs to invests in dedicated cybercrimes courts to hear such matters and attend to the nuances involved. This is however unlikely to change in the foreseeable future.

Craig Pederson
Director, TCG Digital Forensics

Crypto fraud especially is hurting South Korea hard

To counter fraud and money laundering, it is expected that 35 of the 68 crypto-exchanges will be closed in 2021

The **Korean National Police Agency** (KNP) has integrated all reports through its own **Electronic Crime and Report Management System**. Cybercrimes can be reported here as well. The KNP has a separate Cybercrime Bureau where citizens can check for scams and apply for cyber-awareness training.

The KSA works closely with civilian cybersecurity experts and related organizations such as the **Korea Internet & Security Agency** (KISA). KISA's focus lies on strengthening the competitiveness of the Internet in Korea. Their aim is also that of developing and spreading information regarding online security.

The Cheat is an online platform where people can share scam information. It was launched in 2006. Fraud victims can share a total of 10 types of information such as the name, ID, account number, and cell phone number of the fraudster to prevent other consumers from being scammed.

In 2019, the police received 180,499 cybercrime-related reports. 136,074 of these were related to Internet fraud and 10,542 to financial crime. Other crimes were related to hacking, malware, DDOS attacks, adult content, online gambling, defamation and cyberstalking. In phishing alone, 405 billion won was lost from January to August 2019. In 2020, 347,675 fraud-related crimes were reported of which 60% online.

Crypto-related fraud is one of the most serious problems. The police received 42% more reports in 2020 compared to 2019. New legislation is forcing exchanges to obtain licenses from financial and Internet regulators. Until now only 28 exchanges out of the 63 operating in South Korea have received certification from the Korea Internet and Security Agency (KISA), the first step to obtaining final approval from the Financial Services Commission (FSC). The remaining 35 exchanges are unlikely to comply.
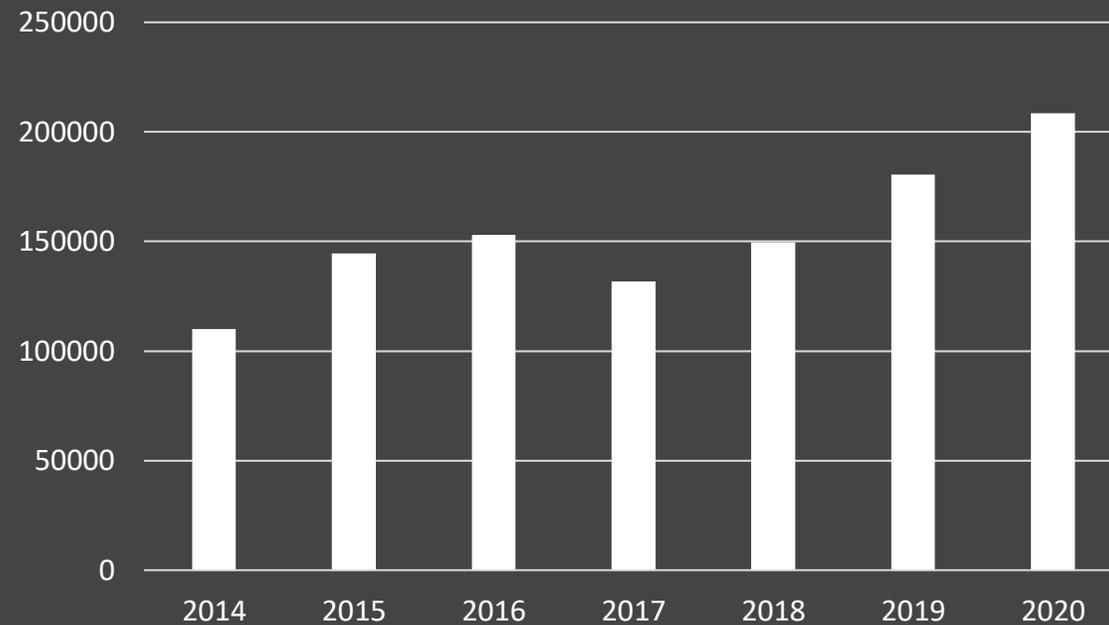
Number of cyber crime cases in South Korea from 2014 to 2019

Key Statistics:

Population:	52 million
Internet:	95%
# of Scams:	208,605* (53%)
Scams / 1,000 :	4.0
Money lost:	€ 388 million*
Per capita:	€ 7,49
Per report:	€ 1.858

Key Organizations:

KNPA KOREAN NATIONAL POLICE AGENCY

KISA KOREA INTERNET & SECURITY AGENCY

World Best! 경찰청 사이버수사국 CYBER BUREAU

THECHEAT

Cybercrime in Spain has risen by 23% during the pandemic

To offer more support, INCIBE has launched a 9AN to 9PM, 365 days a year phone and digital support number: 017

The Spanish **Cybercrime Central Unit of the Guardia Civil** was created in 1996. Nowadays, each of Spain's 17 regions has its own local cybercrime team as well to investigate digital crimes.

The **Spanish National Cybersecurity Institute** (INCIBE), founded in 2006, which reports to the Ministry of Economic Affairs and Digital Transformation, focuses on cybercrime research, the provision of services, and cooperation with relevant actors directed at cybersecurity. This is done both at the national and at the international level.

Consumers can report online fraud both to the local police, the <u>Guardia Civil</u>, and to the <u>National Police</u>, both online and by phone. In addition, INCIBE has launched 017.017, a national, free and confidential cybersecurity service for companies and consumers to help solve cybersecurity problems. 017 is a phone number which can also be reached via Telegram, Whatsapp and online. The service is attended by a multidisciplinary team of experts, who offer technical, psychosocial and legal advice. The service runs from 9AM to 9PM, 365 days a year .

The <u>Association of Spanish Companies Against Fraud</u> was created in 2014 as non-profit organization to coordinate the exchange of anti-fraud knowledge and data to protect both consumers and companies. it also offers consumers information on card and identify fraud, social engineering and other scams.

INCIBE reported 133,155 incidents in 2020. 35% of these were related to malware, 32% to fraud, and 17% to unauthorized access of a system. Reports were filed by more than 106,466 thousand consumers and 1,190 companies.

Chart

Year	Number of cyber incidents reported
2013	8,925
2014	17,885
2015	49,976
2016	115,257
2017	123,064
2018	141,519
2019	107,397
2020	133,151
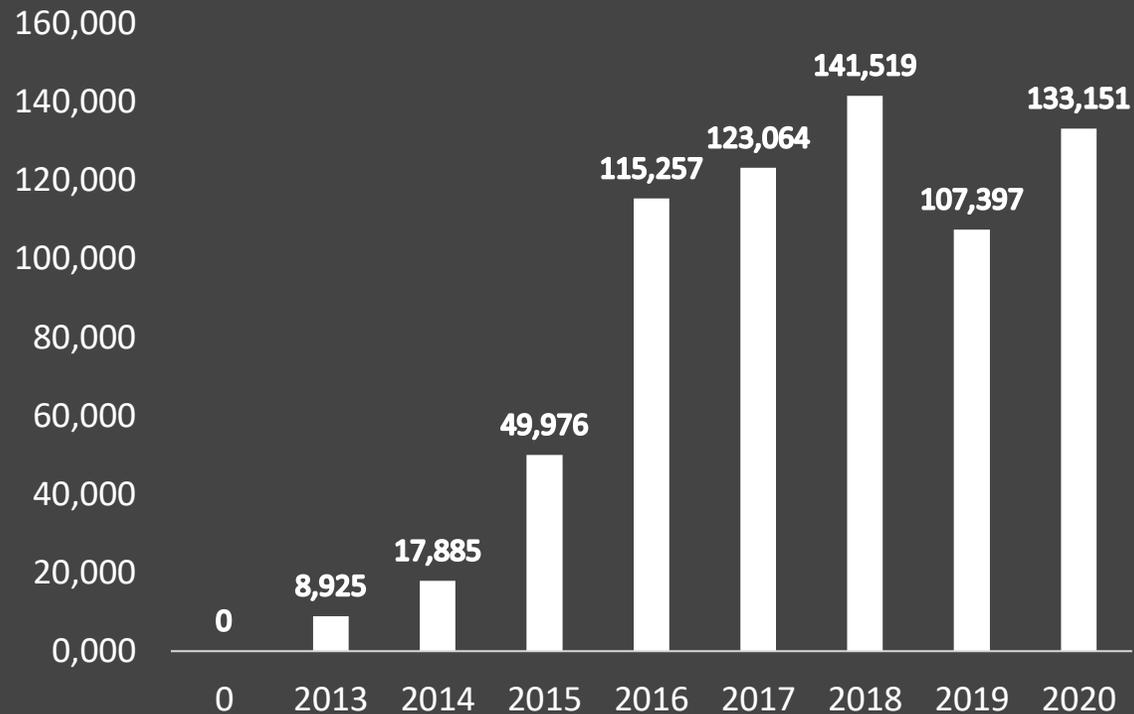
Number of cyber incidents reported, Instituto Nacional de Cibersegundad

Key Statistics:

Population:	47 million
Internet:	91%
# of Scams:	42,610 (23%)
Scams / 1,000 :	0.9
Money lost:	€ 42 million
Per capita:	€ 0,89
Per report:	€ 991*

Key Organizations:

GUARDIA CIVIL — incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD — POLICIA NACIONAL — ccn-cert centro criptológico nacional

*ScamAdviser Expert Estimate

INCIBE offers a cybersecurity hotline to help companies and consumers

In addition, it offers several apps and organizes events to educate and train children and students

017

47.503
Total number of queries answered

39.206
Queries answered by telephone

8.297
Queries answered by mail

TU AYUDA EN
CIBERSEGURIDAD
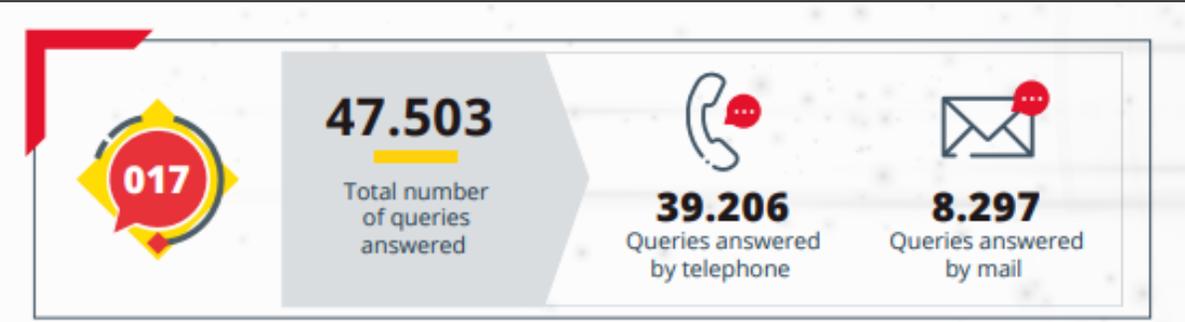
How to contact

Instant messaging

Helpline 017

Web form

OUR EVENTS

CyberSecurity
Summer Bootcamp
Specialist training for FCSE, CERT and Policy Makers

ENISE
The leading event for the cybersecurity sector

Safer Internet Day
Safe and responsible use of technology in the field of minors

OUR APPS

CONAN Mobile
Real-time analysis of security in Android

Hackers vs. Cybercrooks
Learn about security on the Internet by playing with Sergio

Hackend
Play and learn to detect cybersecurity breaches in companies

OSI Oficina de Seguridad del Internauta

79.059
Notices to citizens about the antibotnet service

is4k INTERNET SEGURA FORKIDS

42.866
People participated in
1.754
awareness-raising and training actions in the child's environment

Specialist Training

>1.000
students from
62
countries undergoing specialist training

incibe.es/sites/default/files/paginas/que-hacemos/cybersecurity_balance_2020_incibe.pdf

In Sweden fraud is declining but online fraud is growing

Online scams now constitute 2/3 of all fraud crimes reported

Online fraud can be reported to the **Swedisch police** at their offices, via email or online.

The numbers of reported fraud cases (both online and offline) declined by 11 % from 2019 to 2020 to 218,000 reports. This is primarily due to the decrease in credit card fraud; most other types of fraud increased during 2020. For the first months of 2021 this decrease continued. Online fraud is estimated to now make up 2/3 of all cases.

As a result, online fraud has become a large part of all reported crime. While in 2000 5% of all crimes were fraud related this number was 17% in 2020.

At first glance, the decline in numbers looks positive, but it is the reflection of fraudsters focusing on more profitable types of crime. The average card fraud costs the consumer some 5,000 Swedish krona (€493), while the average romance fraud case costs them over 350,000 Swedish krona (€34,500). These two scams alone have already resulted in a loss of €84 million.

The pandemic has had an impact on fraud development. This includes fraud against individuals (e.g., a large network selling fake PCR results), against companies (e.g., BEC or CEO fraud with Covid 19-themes) and against the state (governmental support for companies in need of financial aid). Most of the fraud types are "old school" scams in new clothes.

bra.se/bra-in-english/home/crime-and-statistics/crime-statistics.html

Fraud Reports — **% of all crime reports**

Key Statistics:
Population: 10.3 million
Internet: 93%
# of Scams: 145,333 (-11%)
Scams / 1,000 :   14.0
Money lost: € 179 million*
Per capita: € 17,34
Per report: € 1.235

Key Organizations:

Swedish Police

Polisen
Swedish Police

Switzerland is especially venerable to investment scams

The amount lost per capita is one of the highest in the world

Switzerland is a confederation of 26 cantons. As a result, Swiss citizens can report online fraud to the police agency of their canton.

The **Nationale Zentrum für Cybersicherheit** (NCSC) is gaining a more central role in reporting online fraud, in the analysis of the phenomenon, and in the prosecution. Both consumers and companies can report any kind of cybercrime to the center, from DDOS attacks and digital extortion to advanced fee fraud. In 2018, the Netzwerks digitale Ermittlungsunterstützung Internetkriminalität (NEDIK) was set up to work closely with NCSC in the collection of cybercrime-related data and the coordination of cybercrime cases across all cantons.

The **Swiss Crime Prevention** (SKP) is an inter-canton specialized agency in the field of prevention. It offers information to consumers on several topics including Internet-related crimes and fraud.

In addition, the **Cyber Crime Police**, an initiative of the Canton police of Zurich, informs German-speaking consumers about online scams and cyber-related incidents. Other cantons are developing special consumer awareness sites as well.

The police received 16,395 cybercrime reports related to fraud in 2020. According to the National Center for Cybersecurity, advanced fee scams remain the most frequently reported type of fraud (20%). Email is still the favorite medium for advanced fee scams.

6% of the reported scams were related to (fake) sextortion 3.7% were fake invoice scams. Most of these were emails announced a non-existing parcel delivery for which custom duties had to be paid - usually for a total amount of CHF 75.00. Other crimes reported were Classified Ads (2,6%), Fake Tech Support (2,3%), and CEO fraud (2%).

REPORTS TO THE NCSC IN THE SECOND SEMESTER OF 2020
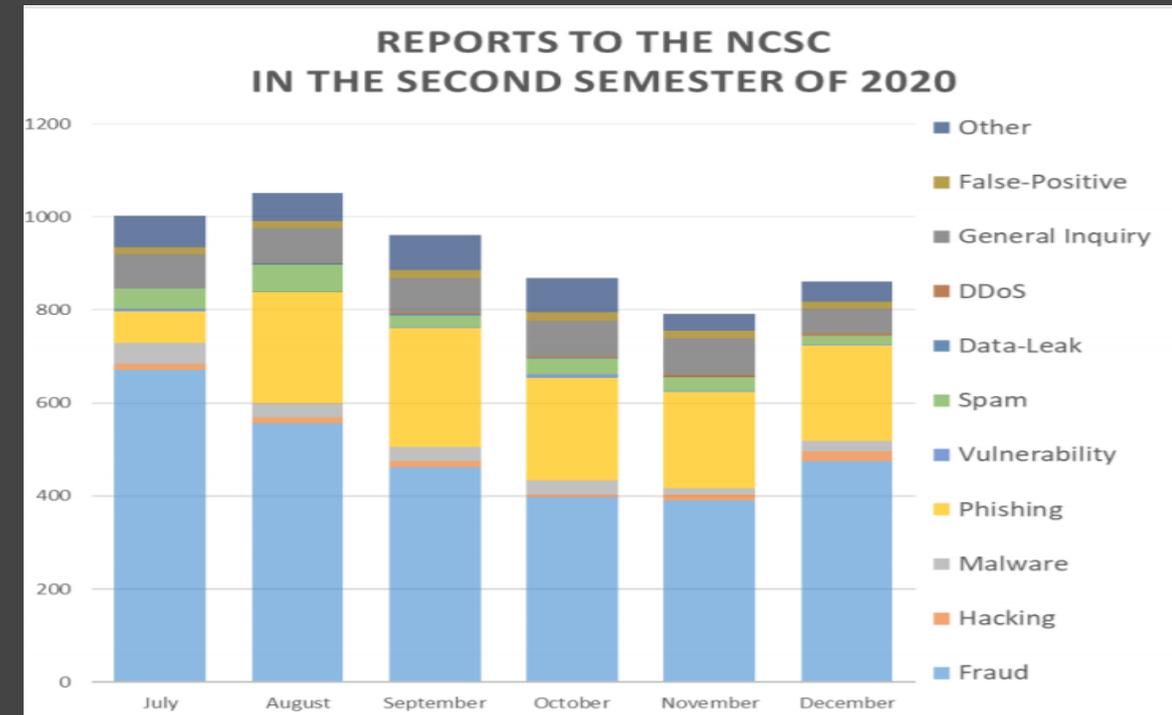
Reports to the NCSC in the second half of 2020

Key Statistics:

Population:	8.6 million
Internet:	93%
# of Scams:	10,694
Scams / 1,000 :	1.2
Money lost:	300 million*
Per capita:	€ 32.04
Per report:	€ 25,874

Key Organizations:

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Nationales Zentrum für Cybersicherheit
NCSC

CYBERCRIMEPOLICE.CH
Ein Engagement Ihrer Polizei

SKPPSC

* ScamAdviser Expert Estimate

In 2021, scams increased by 93% in Taiwan

The police is sharing scam data publicly to help security companies and (social) media warn and protect consumers

Consumers can report scams to the **Taiwan Police Agency**. This can be done via the local police office, via phone, mobile app and online. The police has also launched a **separate website** to warn the public about scams and allow easy reporting. Due to the increase in online fraud, the police is investing strongly publicity. The media is also paying more attention to online fraud and scams are a hot topic on social media.

According to the Taiwan Police, 23,054 frauds were reported in 2020, with 36,952 victims. From January to October 2020, NT$3.1 billion (€94 million) was lost. 22,647 scammers were apprehended.

The top three scams in 2020 where the most money was lost were investment frauds, accounting for 23.67%, followed by imposter scams. Mainly People aged 30 to 33 years were the most susceptible to investment scams. Covid-19 forced people to look for alternative sources of income. In 2020, 670,000 consumers opened a trading account and 47% of Taiwanese consumers now trade. Celebrities have been lured to promote cryptocurrency and other investment scams. Victims were attracted by slogans like "make money without losing money".

The imposter scams mainly target people over 50 years old, where scammers pretended to be a family member in need (7.8%) or a government official demanding payment of a, non-existing, fee (15.7%).

In Q1 of 2021, the top three scams were, investment scams, fake banking phishing, and ID theft. Most scams were carried out via instant messaging services and social media.

Government data is open for the public to learn about anti-scam actions. Since 2018, Trend Micro has used the public data provided by the Taiwan government to provide free and public scam protection services. In 2020, Trend Micro extended these free services to other regions, supporting 15 languages.

Sources: Trend Micro
cna.com.tw/news/asoc/202011010101.aspx
cna.com.tw/news/asoc/202107270043.aspx

Shield Yourself from Online Scams

Trend Micro Check can protect you from scams, phishing attacks, malware, and dangerous links with our leading detection technology.
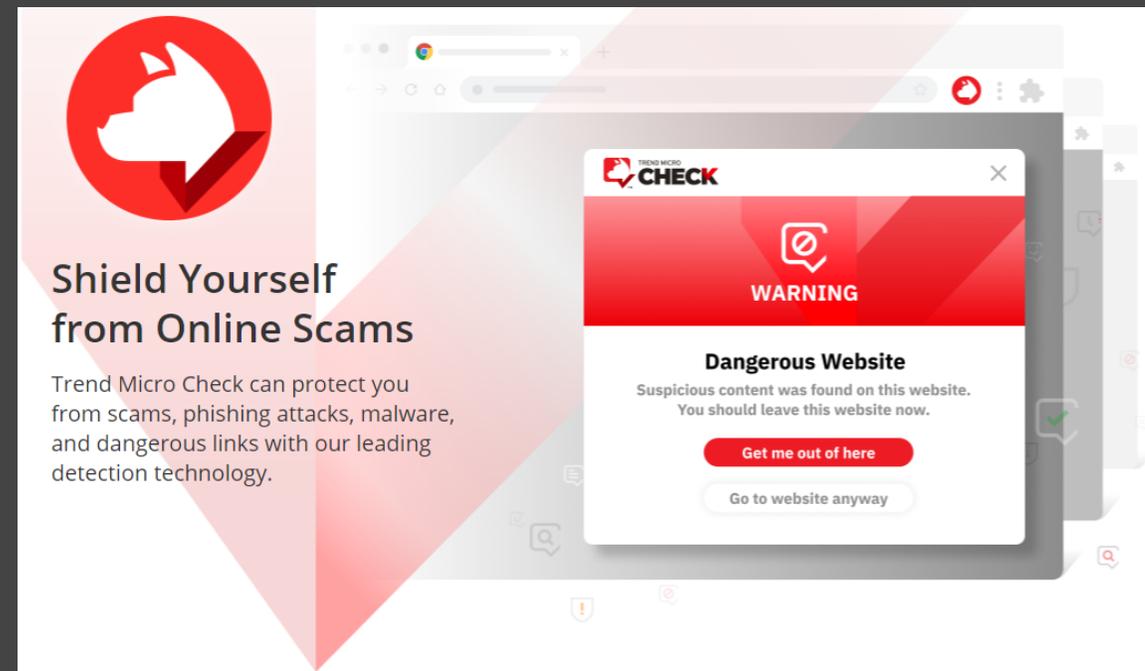
Trend Micro is using open data to fight online scams

Key Statistics:

Population:	23,6 million
Internet:	84%
# of Scams:	23,054 (93%)
Scams / 1,000 :	1.0
Money lost:	€ 94 million
Per capita:	€ 4.00
Per report:	€ 4,092

Key Organizations:

內政部警政署 165全民防騙網
National Police Agency, Ministry of the Interior

In 2020, 7% of Turkish citizens were victims of a cybercrime

Internet use increased by 70% during the pandemic social isolation period

To report cybercrimes, Turkish citizens may apply to the public prosecutor's offices, to the local police or gendarmerie stations (and to their cybercrime units where available) to the Cyber Crimes Department of General Directorate of Security Affairs and to the Presidential Communications Office CİMER. Citizens can physically make reports to the office of a public prosecutor or to local stations by stating their complaint verbally or in writing; they can also use the online module of the police department, or call "155". CİMER complaints are done in writing, online or via post.

According to a study by the Turkish government, 7% of all Turkish citizens fell victim to cybercrime last year. Close to 1% of the respondents became victims of hacking, 1.8% were hit by cyber harassment and cyberbullying, 2.3% was exposed to cyber economic crimes, and 5.1% suffered malware threats.

The **Department of Cybercrime** , part of the Turkish Police, has four divisions: Digital Forensics, Investigation, Prevention and TECOP (technical and operating support). The team works closely together with the provincial police units, preventing duplicate investments and allowing more effective combat against cyber crimes. It also invests heavily in training regional police forces.

The main activities of the Cybercrime Department are fighting cybercrime, raising awareness about cybercrime, increasing international cooperation in the fight against cybercrime, evaluating cybercrime threats against Turkey, training investigative and forensic personnel, and following technological developments to increase its capacity to combat cybercrime.

Social media platforms are especially used by scammers. Hence, the Department of Cybercrime monitors 45 million social media accounts and receives around 3,000 complaints daily. Online prostitution, drugs and betting are the most common cybercrimes followed by insulting state authorities. Most money is lost in cryptocurrency scams. In two scams alone, more than €112 million was lost.

Other organizations involved in fighting cybercrime are the CERT, under the Scientific and Technological Research Council ("TUBITAK")'s Informatics and Information Security Advanced Technologies Research Center ("BILGEM"), the National Cyber Incident Response Center ("USOM"), and the Sectoral and Institutional CERT Teams ("SOME"), under the Information and Communication Technologies Authority. Also operative in this field are **Bilişim Teknolojileri ve Siber Güvenlik Derneği** (Information Technologies and Cyber Security Association) ("BTK") and **Türkiye Bilişim Derneği** (Turkey Information Technologies Association) ("TBD") and **BankalarArasi Kart Merkezi**, which represents 13 banks, warning people about online scams.

Key Statistics:

Population:	84.3 million
Internet:	82%
# of Scams:	1.9 million
Scams / 1,000 :	23
Money lost:	1,136 million
Per capita:	€ 13.47
Per report:	€ 586

Key Organizations:

Cybercrime is under-reported and under-fought in Turkey

Interview with Laçin Özer, Associate at Kılınç Law & Consulting

How would you describe the online scam situation in Turkey?

In recent years, there were several notably widespread online scams in Turkey. One of them, an online game of farming called "Çiftlik Bank", emerged in 2016 and was an online Ponzi scheme that promised that the animals bought and fed in a farm game played on the internet would be used for production in farms established across various Turkish cities. This promising initiative turned out to be a great scheme that caused a total loss of 1 billion, 139 million and 972 thousand Lira, having scammed more than 130 thousand people. Another notable example of an online scam in Turkey happened in the field of coin transactions. A company called Thodex, an online cryptocurrency trading platform, scammed consumers and investors. The total loss is estimated to be between 108 million USD and 2 billion USD.

Given the surge in phone scams in Turkey in the last decade, which is now continuing on online platforms, there have been several initiatives taken by public and private institutions to raise awareness in communities and help consumers and citizens detect possible fraudulent activities. Public authorities and nationwide media outlets seem to play a pivotal role when it comes to raising awareness.

Which actions are working against scammers in Turkey?

Awareness-building worked positively in the past in Turkey. This resulted in less phone scams, and one might say that this approach is yielding positive results in online scams as well. Furthermore, two significant examples of online scams and the legal actions taken against them have helped to raise awareness among consumers. It is important to note the efforts of the specialist units within the police and gendarmerie force in preventing scams and cybercrimes, as well as the endeavors of non-governmental organizations. Although it is early to say, the results of these two big legal cases may help to decrease the number of new online scam activities.

Laçin Özer
Associate at Kılınç Law & Consulting

Scams increased by 6.5% in the United Kingdom

The amount lost increased from £ 2,3 billion to £ 2,35, an increase of 16.7%.

Action Fraud is the UK's national reporting center for fraud and cybercrime. The service is run by the **City of London Police** working alongside the **National Fraud Intelligence Bureau (NFIB),** responsible for assessment of the reports. The City of London Police is the national policing lead for economic online crime.

Between July 2020 and June 2021, the NFIB reported 875,622 cases of fraud and £2.35 billion lost, received a.o. from ActionFraud, Cifas and UK Finance (unclear). 80% of fraud is now cyber enabled. This is a growth of 6.5% in number of reports and 16.7% in money lost from July 2019 to June 2020.

The most reported fraud types, excluding the category labelled "other", are Cheque, Plastic Card & Bank Account (336,707), Online Shopping and Auctions Fraud (103,254) and Application Fraud (91,593).

The largest amount of money was lost in Investment (£318m) Cheque, Plastic Card and Online Bank Accounts (£184m) and Share Sales or Boiler Room Fraud (£171m).

The highest harm threats for 2021-2022 are frauds linked to Courier, Romance, Payment Diversion, Investment, Computer Software Service and frauds linked to Card and Online Bank Accounts.

Money mules persistently feature across most fraud types while social media and encrypted messaging services increasingly act as enablers.

colpolice.maps.arcgis.com/apps/opsdashboard/index.html
https://www.actionfraud.police.uk/fraud-stats

Reported

Public Sector Fraud	
Investment Fraud	
Courier Fraud	
Banking Fraud	
Other Fraud	
Cyber Dependent Crime	
Corporate Fraud	
Consumer Fraud	
Advance Fee Fraud	

0   50000   100000   150000   200000
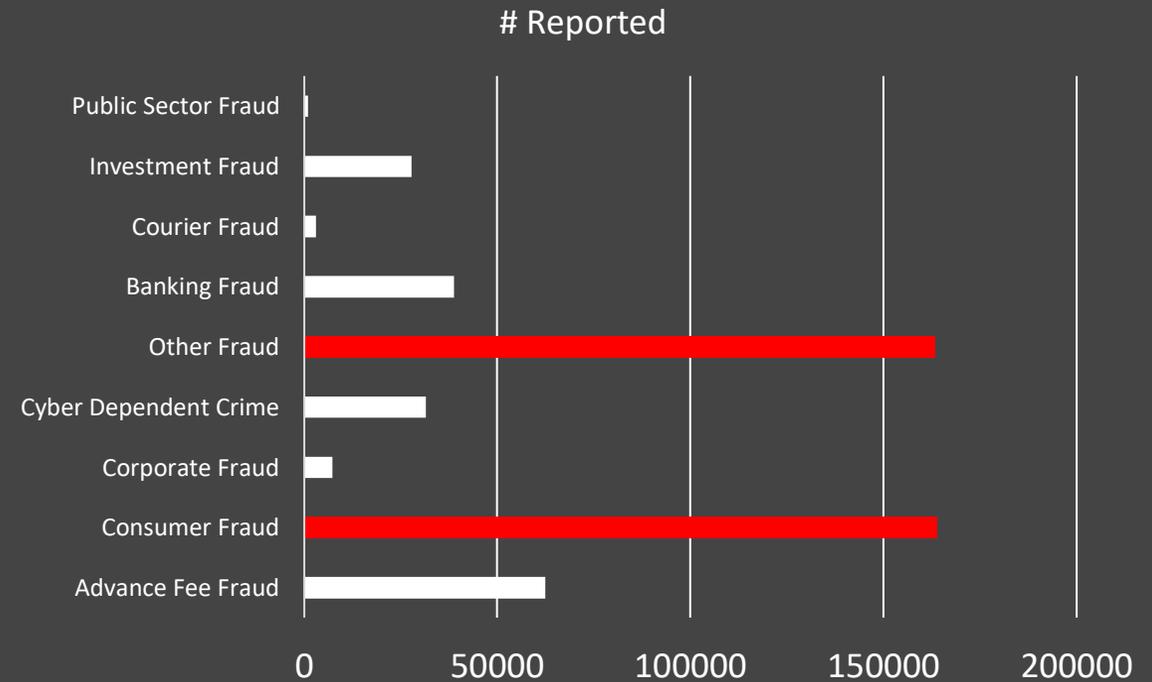
Key Statistics:

Population:	67 million
Internet:	95%
# of Scams:	875,622 (6.5%)
Scams / 1,000 :	13
Money lost:	€ 2,001 million
Per capita:	€ 29.77
Per report:	€ 2,285

Key Organizations:

CITY OF LONDON POLICE

ActionFraud
National Fraud & Cyber Crime Reporting Centre
actionfraud.police.uk

Other cybercrime-related organizations in the UK

Apart from the London Police, there are several other organization involved in cybercrime awareness and combating

The **National Trading Standards eCrime Team** (NTSeT) monitors and investigates several online consumer and business frauds including website dating scams, misleading websites, subscription traps, and online shopping frauds. NTSeT is the owner of the **Friends Against Scams** initiative which aims to protect and prevent people from becoming victims of scams by empowering them to take a stand against scams. More than half a million people have registered as a Friend Against Scams. They are offered a short awareness session in person or online training and are asked to build awareness with their neighbors, friends and family.

Get Safe Online is a public-private sector partnership supported by organizations in banking, retail, internet security, and other sectors. Its website offers information on online safety. In addition, it organizes national events - such as Get Safe Online week - and works with law enforcement agencies and other bodies in support of their outreach activity, internal awareness, and customer online safety.

The **National Cyber Security Centre** was launched in 2016 and has as its mission that of making the UK the safest place to live and work online. The center supports the most critical organizations in the UK, the wider public sector, industry, SMEs, and the general public. They maintain the website Cyber Aware to inform consumers about the actions they can take to ensure that they use the Internet safely.

The **National Crime Agency** fights serious and organized crime threats including cybercrime and fraud. Key partners include the Serious Fraud Office, the City of London Police, the Metropolitan Police Service, the Financial Conduct Authority, and the National Cyber Security Centre.

The UK is on the front-line; we get the newest scams first

Interview with Andy Bates, Chief Development and Strategic Partnership Officer at Global Cyber Alliance

You work internationally but live in the UK. How would you describe the "scam market" in the UK?

Unfortunately, I tend to think that the UK is ahead of many countries in that we get to see some bad scams before everyone else. The big one we see a lot of is the parcel delivery scams where people receive messages such as "Hey, this is the post office, pay £3.99 for customs and you parcel will be delivered tomorrow!". This is effective as no one tends to call the police for £3.99. Smishing and sequential dialing is also very prominent. Personally, I almost never answer my landline if i don't know who is calling me. It's however soul destroying for many people.

Where do you think the UK is leading the fighting against scams? Where can things be improved?

There are several UK industry-lead coalitions. STOP SCAMS UK for example, is a collection of banks and telecom operators, who work together to stop scams before they cause harm. The Global Cyber Alliance works with them on the "DIAL 159" campaign. If we look at a UK-USA cooperation the "7726 for SPAM" is an excellent project. In this scheme consumers are invited to forward phishing texts to 7726.

How can we make the world a safer place and what's the role of the GCA in it?

My obvious answer is the DomainTrust platform which we launched in 2020. DomainTrust allows people to share information regarding malicious and suspicious domains, which helps registries and telecom operators take down or block these domains. This platform is gathering pace with 2 million domains now listed and some material domains being taken down. The Global Cyber Alliance's internet integrity program looks at these kinds of infrastructure-based projects helping to be a neutral NGO "broker" between commercial companies, NGOs, and government agencies around the world.

Andy Bates
Chief Development and Strategic Partnership Officer
Global Cyber Alliance

The United States remains the country most hit by online scams

The largest amount of money is lost by early retirement seekers and in imposter scams

Americans can report online fraud to multiple agencies. From local law enforcement, to credit card companies and PayPal, the **Better Business Bureau**, **FBI IC3** or the **Federal Trade Commission** (FTC).

In 2020, the FTC received 4,7 million reports from consumers and the above-named organizations. Via its Consumer Sentinel Network, the data is shared with 3,000 federal, state, and local law enforcers across the country.

2,26 million reports were related to fraud and $3.3 billion was reported lost (up from $1.8 billion in 2019). 34% of the reporters lost money, up from 23% in 2019.

1,4 million consumers reported identity theft, about twice as many as in 2019. 406,375 reports came from people who said their information was misused to apply for a government document or benefit, such as unemployment insurance. This was a huge increase from 2019, when the number was 23,213.

According to the FTC, the most common scams were imposter scams (500,000 reports, $1.2 billion lost, with an average loss of $850). Government and business imposter scams were also among the top categories of COVID-19 and stimulus-related reports.

Online shopping and negative reviews was the second most reported fraud category (350,000 reports) of 2020 with online stores delivering extremely late or not at all. $245 million was reported lost, with an average loss of $100. Internet services, prizes, sweepstakes, otteries, and telephone and mobile services rounded out the top five fraud categories. The phone (increasingly text messages) is the most common medium used by scammers. The most commonly misused payment methods are gift cards and reload cards.
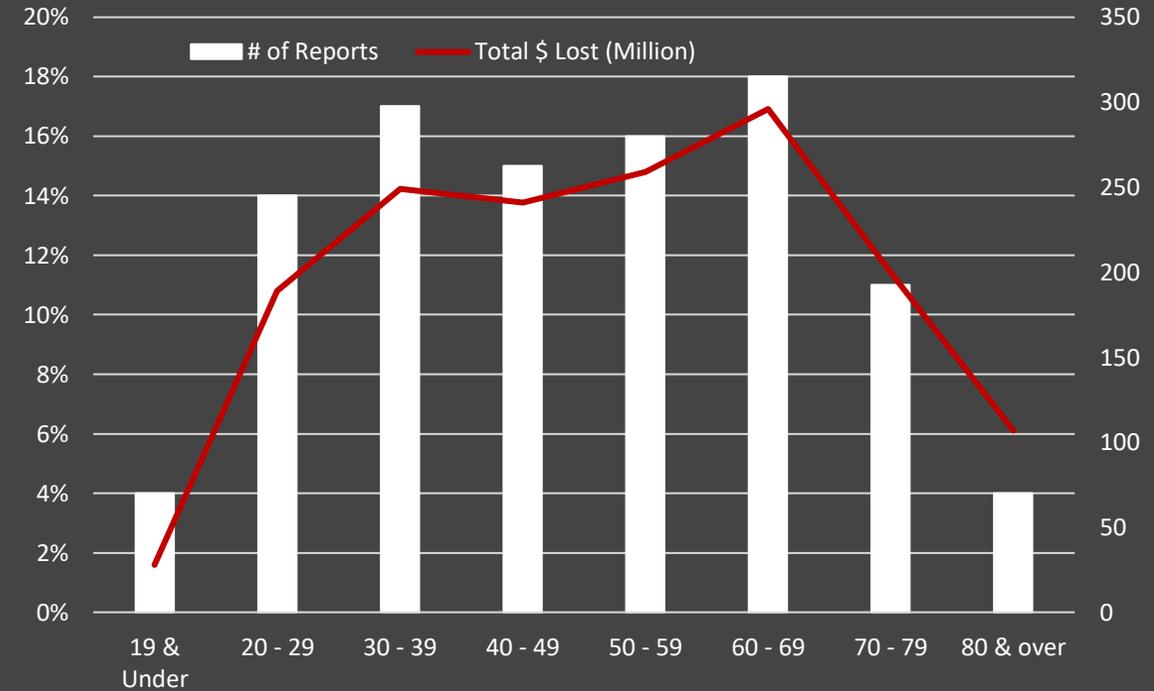
Key Statistics:

Population:	330 million
Internet:	95%
# of Scams:	2.26 mill. (22%)
Scams / 1,000 :	6.7
Money lost:	€ 2.815 million
Per capita:	€ 8.55
Per report:	€ 1,280

Key Organizations:

We need to cooperate more intensively on a global level

Interview with Donna Gregory, Unit Chief, Internet Crime Complaint Center (IC3), Federal Bureau of Investigation

How do you see the "scam industry" developing in the USA?

During the pandemic, we have seen a huge increase in reporting; however, from that reporting the IC3 does not necessarily see new scams but new twists to old scams. Although phishing schemes remain high on the list of reported activity, the predominant cyber scams we are currently seeing are Business Email Compromise (BEC), Ransomware, Tech Support schemes and SIM Swapping.

How is the FBI working on consumer awareness, next to reporting?

This year the IC3 published 37 publications for consumer and private sector awareness to include 11 public service announcements, 24 Industry Alerts , and the release of our IC3 Annual Report and the IC3 Elder Fraud Report. We develop these publications in conjunction with our National Press Office to get these alerts attention in the press and to consumers.

Which 'anti-scam' actions did the FBI undertake in 2020?

I can only speak for the IC3 actions. Our biggest success, remains the recovery efforts related to BEC and other financial frauds. In 2020 we were able to help freeze over $380 million and 2021 looks to be even a "better" year. To date, since 2018, we have worked with our financial service partners to freeze more than $825 million related to BEC and financial scams.

Which actions should we, as global community, undertake to fight scams better?

The most effective action is collaboration at a global level. We all are victims of the same cyber scams, as cybercrime has no boundaries. Regardless of where we are located across the globe, our citizens are suffering losses, and the cybercriminals who receive these funds are from all over the world. Law enforcement needs to work more intensively together on a global level, the private sector needs to be involved as well, and victims need to report the activity. The combination of all three is the only way we are going to effectively combat these criminal groups.

Ukraine reported a Cybercrime increase of 2.5% in 5 years

Ukraine traditionally suffers from corruption and fraud and online scams have been a logical replacement during Covid-19

The **Cyber Police Department** was established in 2015 as part of the National Police of Ukraine, reporting to the Ministry of Internal Affairs. The department is comprised of approximately 400 law enforcement officers and senior specialists, including officers employed in every region of Ukraine at local cybercrime units.

The goal of the Cyber Police Department is to detect and investigate all crimes committed by via ICT, including computer-related fraud, crimes on the Internet, child abuse, and infringement of copyright.

In order to collect and analyze electronic evidence, the Cyber Police Department engages experts of the Forensic Science Centre of the Ministry of Interior. The experts take part in collecting, seizing, storing, analyzing, examining and providing expert evaluation of digital evidence.

Ukrainian citizens can report online scams directly at Cyberpolice.gov.ua; this can also be done by phone. The most common type of scams are banking scams when the victim receive a call from "a bank representative" asking for the CVV or PIN code of the credit/banking card.

In 2020 the Cyberpolice received 41,568 reports from the citizens, 80% of which concerned online scams. They blocked 28,859 URLs and 8,798 related bank accounts. The National Police 2020 annual report 2020 mentions 5,000 cybercrimes were registered.

Consumer awareness is one of the biggest challenges. Together with the Ministry of Culture, the Ukraine Cyber Police has developed an educational series to boost cybercrime awareness covering topics like phishing and SIM card fraud.
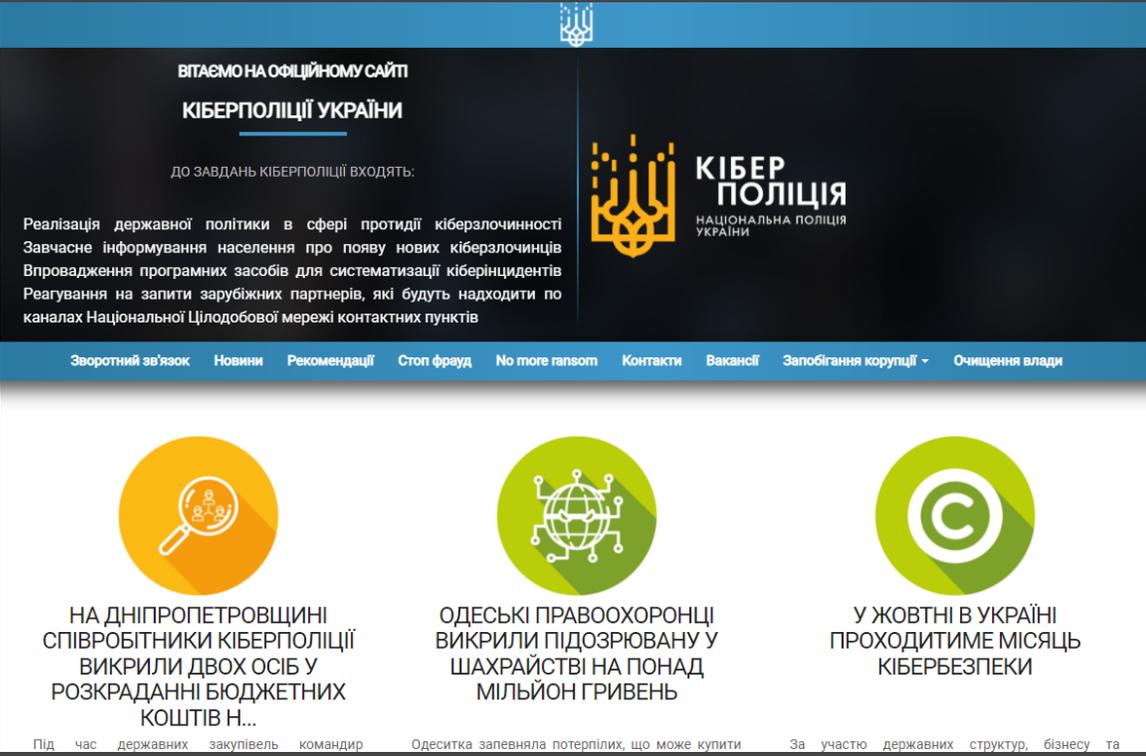
kmu.gov.ua/storage/app/sites/1/17-civik-2018/zvit2020/npu-zvit-2020.pdf
cyberpolice.gov.ua/news/u--roczi-do-kiberpolicziyi-nadijshlo-ponad--tysyach-zvernen-shhodo-shaxrajstva-v-interneti-8412/

Key Statistics:

Population:	44 million
Internet:	93%
# of Scams:	352,000
Scams / 1,000 :	7.98
Money lost:	115 million*
Per capita:	€ 2,61
Per report:	€ 327

Key Organizations:

Ukraine Cyber Police

* ScamAdviser Expert Estimate

Vietnam suffers the most from phishing in Southeast Asia

While the number of cyber attacks decreased, phishing attempts and online scams grew sharply

Several public and private organizations are involved in scam-fighting in Vietnam. The **National Cyber Security Center** (NCSC) focuses on the safety of Vietnam's internet infrastructure, but the center also receives scam reports. **TINGIA** combats fake news and is maintained by the Ministry of Radio, TV en Electronic Information. In addition, there are several private initiatives through which consumers can search and report online scams, such as **Chong Lua Dao**, **Coc Coc** and **ScamVN.**

Vietnam led in Southeast Asia in terms of the number of phishing attacks in the first half of 2020. Vietnam accounted for 464,300 cases, followed by Indonesia (406,200) and Malaysia (269,500); this reflected an increase of 39% compared to 2019.

The most common phishing attempts included using information about the novel Coronavirus as bait, swindling people by offering to sell masks, seeking donations for vaccine research, and offering relief payments.

Next to phishing, Vietnam recorded 2,017 cyber attacks on its information systems in the first half of 2020, down 27.1% compared to the previous year, as reported by the Ministry of Information and Communications' Department of Information Security.

According to the Department of Justice, scams are now the most common kind of crime. The most common types of scams in Vietnam are: 1) Financial scams (investment platforms, online game sites, exchange channels). 2) Identity theft. 2) Romantic scams which often occur via popular social media channels such as Zalo and Facebook.

In 2020, 46,512 websites were reported to Coc Coc, ScamVN and to Chong Lua Dao, and 22,518 websites were blacklisted.

Blacklisted Websites on Chong Lua Dao

Pie chart values: 7%, 5%, 6%, 17%, 65%
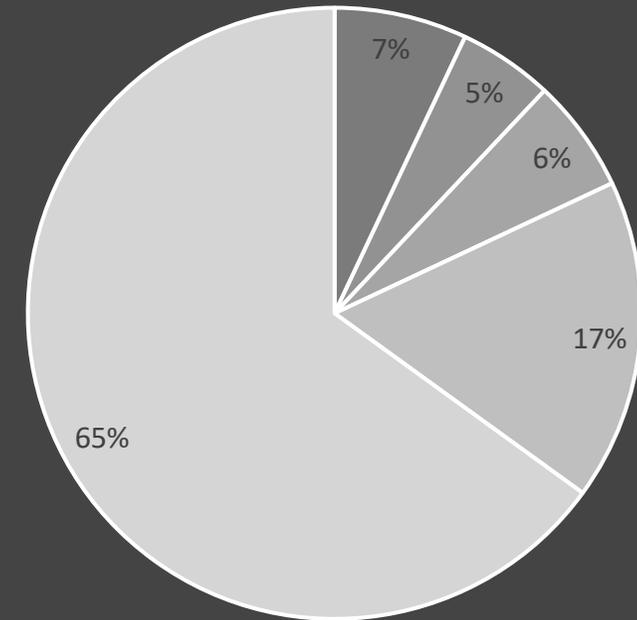
Key Statistics:

Population:	97 million
Internet:	70%
# of Scams:	76155 (39%)
Scams / 1,000 :	0,78
Money lost:	€ 197 million
Per capita:	€ 2,02
Per report:	€ 2,587

Key Organizations:

NCSC VN — National Cyber Security Center

CHỐNG Lừa Đảo — An Toàn Trong Tầm Tay

FAKE

SCAM ALERT SCAMVN.COM

CỐC CỐC

About this Report

About ScamAdviser & The Author

Jorij Abraham
General Manager

Jorij Abraham has been active in the ecommerce community since 1997. He was an Ecommerce manager at de Bijenkorf, TUI and Sanoma Media and Director of Consulting at Unic.

He has been Research Director at Ecommerce Europe & Thuiswinkel.org (the Dutch and European Ecommerce Association). He is professor at TIO University and General Manager of the Ecommerce Foundation & ScamAdviser

ScamAdviser

ScamAdviser helps over 3 million consumers every month to discover if a website is legitimate or a possible scam using an advanced AI algorithm.

Every month, ScamAdviser scans 1 million new domains. Its data is used by anti-virus companies, browsers and internet filters to protect more than 1 billion consumers worldwide.

Feedback is greatly appreciated. You can contact us at report@scamadviser.com