# F-Secured

## Your complete guide to online security in 2023

- Uncover the top cyber security risks
- Learn how to deal with threats
- Discover the hottest security trends
- Get the malware lowdown for 2023
- And much more inside!

F-Secure®

# Executive summary

**The F-Secured guide provides a comprehensive overview of the cyber security threats facing consumers in 2023. But we need to address these issues in a way that people can relate to, because, in the words of F-Secure CEO Timo Laaksonen: "Consumers find protecting their digital moments far too complex and confusing."**

**And so the F-Secured guide focuses on delivering accessible, consumer-focused advice and insight, supported by comprehensive expertise from multiple experts at F-Secure. Key topics in the F-Secured guide include:**

**MALWARE AND INFOSTEALERS.** We review the current malware outlook for 2023, where campaigns will be dominated by information stealing malware (with 69% of the top 30 malware threats we observed in 2022 being information stealers, also known as 'infostealers').

**SECURITY AND THE SMART HOME.** According to Statista, by 2025 the number of connected devices in the average household will hit 34. This increase in connected devices poses a number of challenges for consumers, hardware manufacturers, and CSPs (communication service providers). We review these challenges with Tom Gaffney, a connected home expert at F-Secure.

**PHISHING FOR NEW VICTIMS.** Phishing is an ever-present threat, and whilst it continues to be an effective route for cyber criminals, they are always looking for  new areas to exploit. In the F-Secured guide we review the emerging trends for 2023, with a focus on how gaming and social media are providing new opportunities for scammers.

**CYBER SECURITY IS GETTING PERSONAL.** F-Secure's threat intelligence lead, Laura Kankaala, looks at the increasing issue of relationship dynamics in cyber security, with a focus on stalkerware and security issues that arise from changing personal circumstances. As Kankaala notes: "We are exposing ourselves to new kinds of tracking and privacy related concerns."

**TRENDS AND PREDICTIONS FOR 2023.** With a dedicated team of researchers, analysts, and threat hunters working behind the scenes, F-Secure operates at the leading edge of cyber security. And on this guide we have spoken to some of the company's brightest minds, showcasing their trends and predictions for 2023.

# Contents



# Malware today

Malware. It's the threat that has been pestering us for decades. And here we take a look at the current outlook.

Malware, or malicious software, is an umbrella term for all kinds of software intended to cause harm. Criminals and some government organizations across the globe use malware to spy on people and systems, to steal data, personal details and passwords, and to damage devices and systems. Some of the most alarming modern malware, with many functionalities, can be used for highly sophisticated attacks. Computer viruses, trojans, ransomware, worms, spyware, etc. are all malware.

## Malware in 2022

When looking at 2022 as a whole, stealing information and using it for financial gain was a prevalent threat to consumers. Among many other ways, criminals profit from stolen information by selling personal details and credit card numbers to other criminals; using stolen data for identity theft; hijacking accounts; and using the information, such as bank credentials, to directly steal money.

These goals were also fueling malware operators in 2022. On Windows, the malware campaigns which directly affected consumers mostly involved delivery of information stealing malware. In fact, 69% of the top 30 malware threats we observed were information stealers, also known as infostealers. And 28% were Trojan downloaders, which aim to download other malware. (Source: 'Windows threat type distribution' on page 13.)

## Information stealers

Information stealers do what the name suggests. Once installed, they collect information from the victim's device. This includes data stored on browsers, like saved passwords and auto-fill data, system information, what software the device is running, email credentials, and more. Some variants of information stealers are capable

# “RedLine Stealer was one of the most popular malware tools.”

of capturing screenshots, keystrokes, and even hijacking cryptocurrency wallets.

Through 2022 malware was spread using current events and topics as lures, such as Covid-19, NFTs and Windows 11. Gaming-related lures, such as cheat code files, links to sites for installing computer performance enhancing software, cracks for popular software, and shareware sites were also heavily used to spread malware. The lures were spread in email, websites, links in YouTube videos, and in social media channels like Discord.

## RedLine Stealer

One of the most notable and prevalent information stealers that was actively distributed throughout 2022 was RedLine Stealer. It is a good example of a modern malware-as-a-service business model. Someone creates a piece of malware and then sells it to other criminals, who can then use it for their own purposes. The creator profits without having to spread the malware themselves, which they of course can also do. And when they have the option to simply buy it online, criminals without the capability or skills to create effective malware can use an off-the-shelf version to launch their own malware attacks.

Through 2022 RedLine Stealer was one of the most popular malware tools offered in the dark web marketplaces. One of its benefits for criminals is that this malware is modular: buyers can choose what capabilities they want to use. The price ranges from $100-$800 depending on the subscriptions and offerings. (You can read more about RedLine Stealer on page 13.)

## Ransomware

In 2022, ransomware operators continued to concentrate their efforts on organizations, such as schools, universities, government

entities, medical institutions, and so on. And during 2022, only 1% of blocked malware threats were ransomware (in F-Secure's top 30 malware threats).

However, this does not mean that ransomware poses no threat to online users, as the attacks often involve data exfiltration. This places user data at risk of being breached and sold on the dark web. And while ransomware was not a major direct threat to consumers in 2022, it has not vanished either.

## Mobile malware

Based on F-Secure data, there was a rise in mobile threat infection hits from 2021 to 2022 on the Android operating system. Some of these threats were malicious apps in the Google Play Store. These apps were imitating popular and free apps to lure users to install malware, like banking trojans.

Another notable distribution channel was hiding a trojan inside unofficial versions of popular apps. These apps were promoted with advertisements shown in free and commonly used apps. Following the link and installing the app from an unofficial app store resulted in malware infection. (You can read more about one such Trojan, known as Triada, on page 17.)

And 66% of the mobile malware detections in 2022 were PUAs (potentially unwanted applications). While not always malware, these apps can perform unwanted tasks, such as collecting information or showing ads. They can pose a risk to your privacy and sometimes include malicious modules. Potentially Unwanted Applications often come bundled with another app and work with the same app permissions.

**"66% of the mobile malware detections in 2022 were PUAs."**

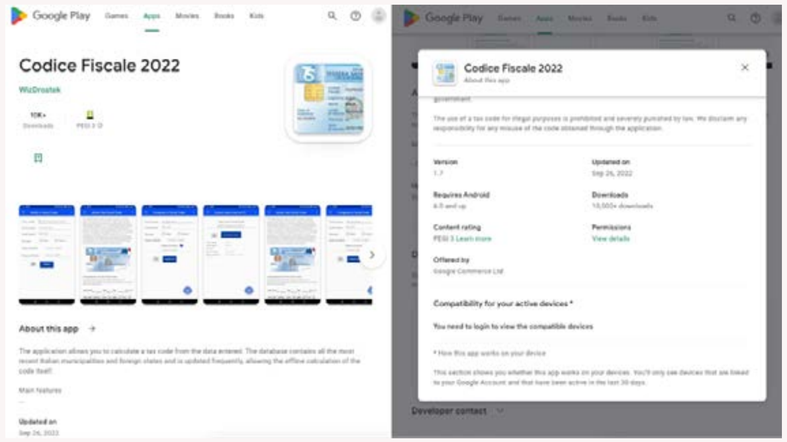
## SharkBot banking trojan

While Google Play tries to filter malware, some get through. In 2022 Google Play Store was a popular channel for distributing malicious apps, like banking Trojans. They aim to intercept your banking information which criminals can use to steal money.

SharkBot was one of the notable mobile banking trojans distributed in Google Play Store. It was posing as different kinds of security and utility apps, like antivirus, cleaners, or file manager apps. SharkBot was spread in the UK, Germany, Italy, Spain, Poland, Austria, the US, and Australia.

(One example targeted Italian users. In this campaign SharkBot was posing as a fake tax code calculator. As the final stage of this attack, the user was asked to update the app. This update downloaded SharkBot, and it took place right after the app was installed.)

SharkBot, like many other banking Trojans, can show a screen overlay on top of actual banking apps. These overlays can look identical to actual banking apps, and it can be very difficult for the victim to realize what's happening.




SharkBot posing as an app for calculating tax code in Italy

(Source: Threat Fabric.)

## Looking towards 2023

F-Secure kept users safe from all of the above threats in 2022. If you don't yet have it, now is a good time to get protected.

As Maria Dacuno, Senior Researcher at F-Secure puts it: "Threat actors will continue to target information or any data that they can use for financial gain."

Therefore, it's more than likely that in 2023 (and further) we will be seeing more infostealers and scams that try to trick you.

# 7 malware tips

Recommendations for staying safe against malware.

## 1 MOBILE MALWARE

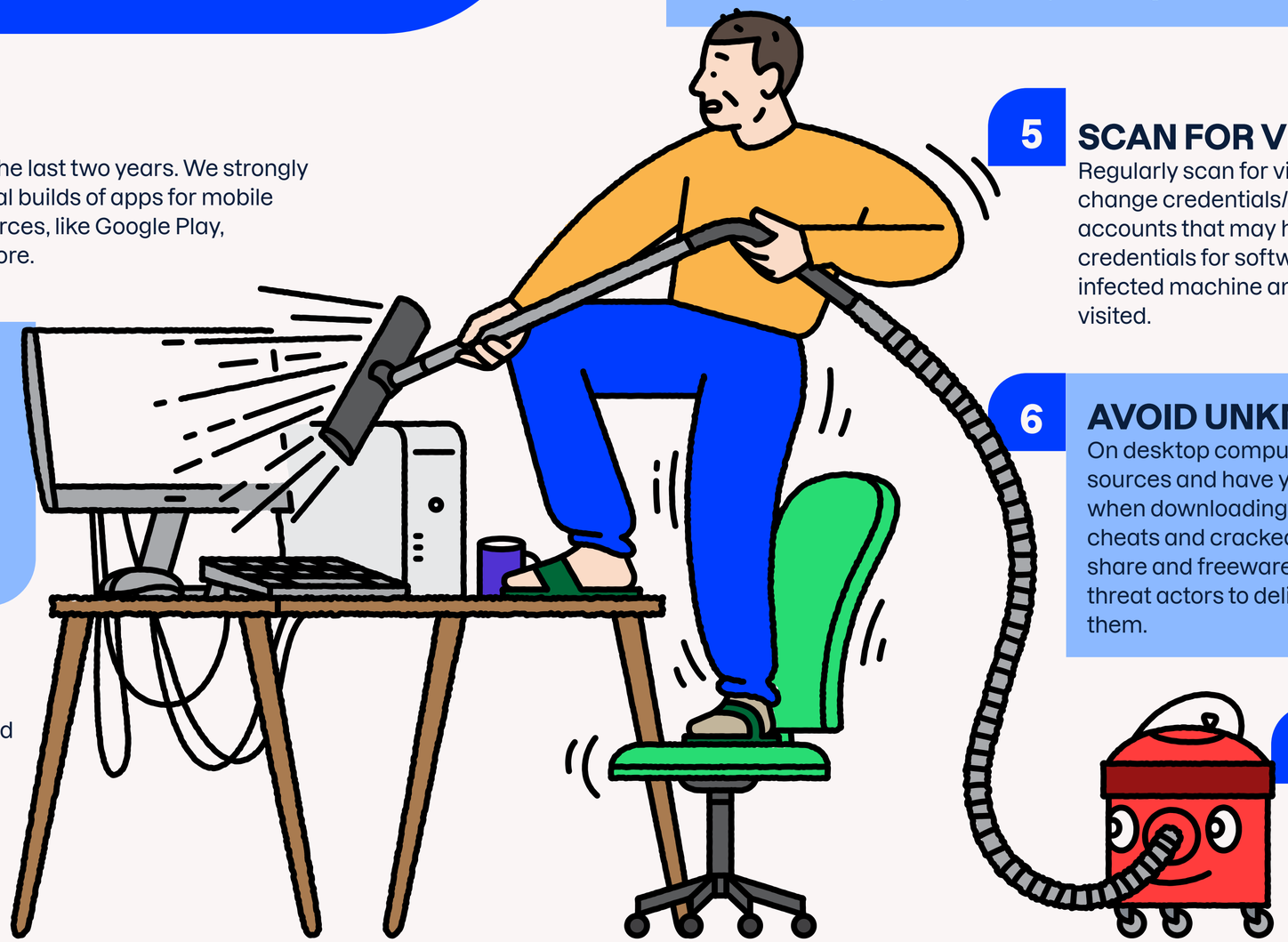
Mobile malware has been on the rise for the last two years. We strongly recommend that you avoid using unofficial builds of apps for mobile devices. Install apps only from official sources, like Google Play, Samsung Galaxy Store and Apple App Store.

## 2 CHECK REVIEWS

Be on your guard also in official app stores. Check the user reviews and look for fake comments. An app with only 5-star reviews and very poor reviews could possibly mean that the users have experienced some unusual or bad activities after installation.

## 3 SCAN REGULARLY

Use reputable security and utility apps and scan regularly to make sure no malware infection is found. If the scan detects an infection, make sure to uninstall the malicious app. Don't use the device for financial transactions and don't use banking apps on the device.



## 4 PREVENT INFECTION

Malware usually tries to avoid detection, so it won't be removed. Therefore, it is always easier to prevent malware infection than to deal with one. Avoiding risks, like unknown links, attachments and applications, and using an internet security solution are the best ways you can protect yourself against malware.

## 5 SCAN FOR VIRUSES

Regularly scan for viruses. If it finds an infection, change credentials/passwords immediately for accounts that may have been stolen, such as credentials for software clients installed on the infected machine and online services you have visited.

## 6 AVOID UNKNOWN SOURCES

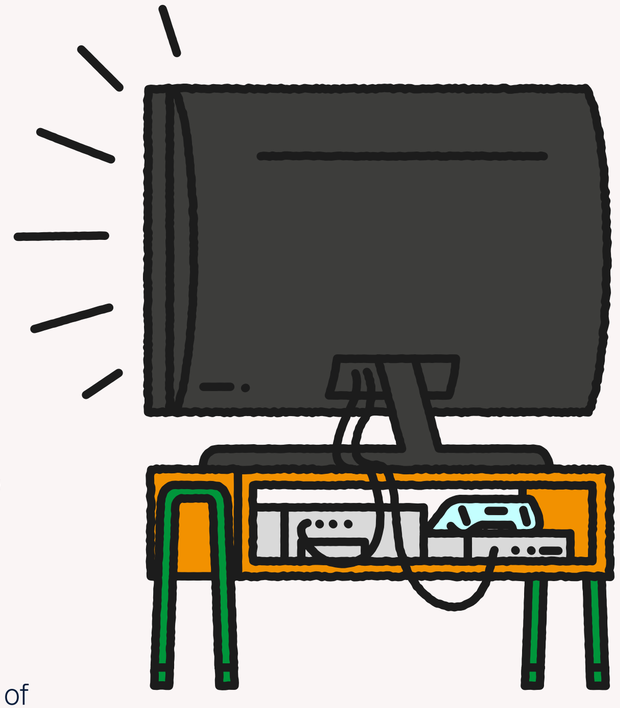
On desktop computers, also avoid unknown sources and have your internet security ready when downloading and installing. Avoid game cheats and cracked and pirated installers on share and freeware sites, as it's common for threat actors to deliver trojans hidden within them.

## 7 NO AUTO-FILL

Avoid saving information to your browser auto-fill settings, as these are common targets for information stealers.

# The connected home and security in 2023

In this Q&A we speak to **Tom Gaffney**, who plays a critical role in promoting F-Secure's Connected Home Security initiative.

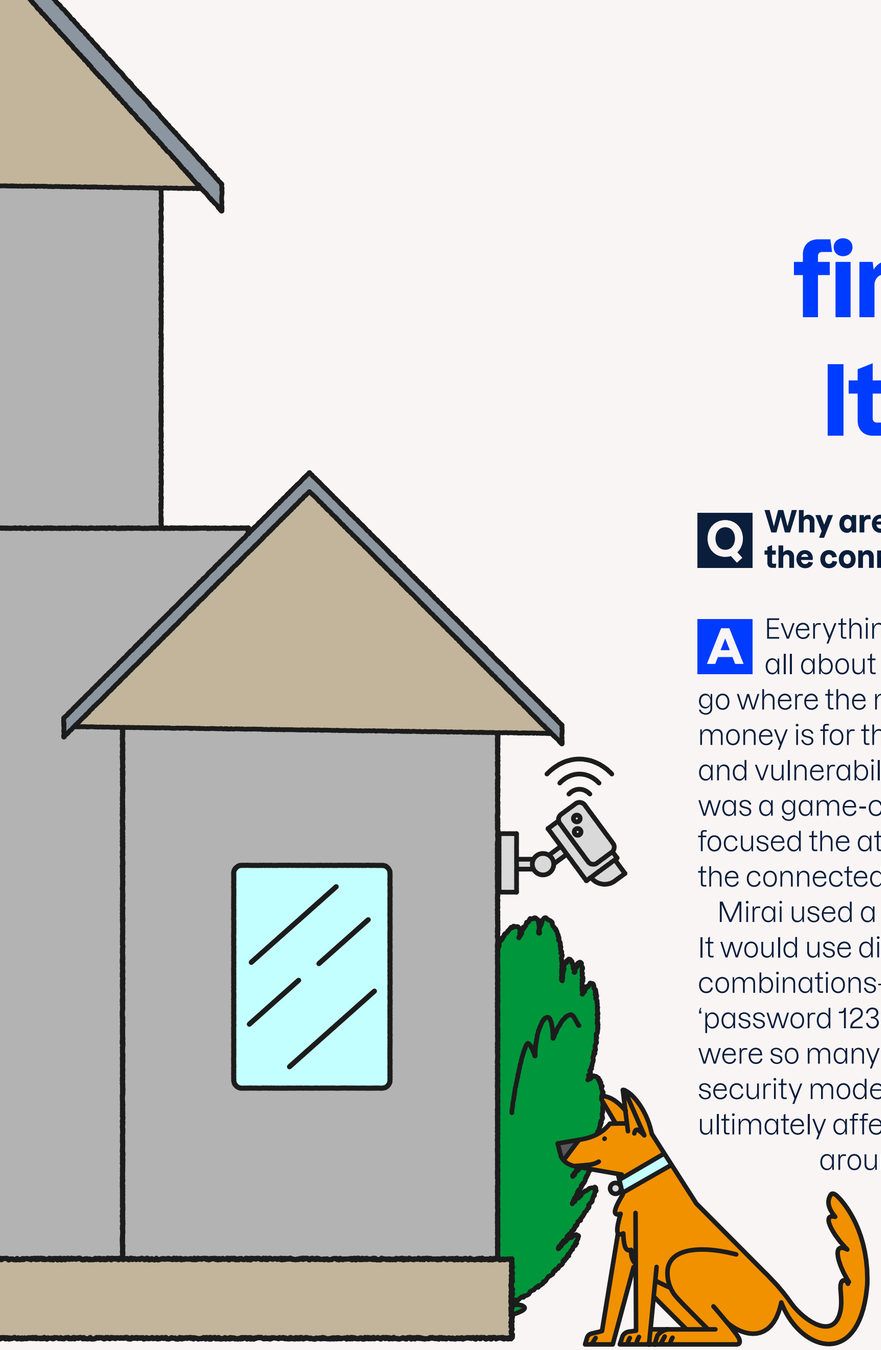


According to Deloitte there are now 22 connected IoT (internet of things) devices in the average home within the United States. And analysts believe this number will continue to increase, with Statista claiming that by 2025 the number of connected devices in the average household will hit 34 (Source: Statista).

This increase in connected devices poses a number of challenges for consumers, hardware manufacturers, and CSPs (communication service providers). And, in the wake of 2016's infamous 'Mirai' botnet, which infected over 600,000 IoT devices at its peak, security is now an ever-present concern in the connected home.

In this Q&A, we speak to Tom Gaffney about the emerging importance of protecting our IoT devices. Gaffney has spent a decade working at F-Secure, serving in various technical and customer experience positions, and he now plays a critical role in promoting F-Secure's Connected Home Security initiative.

Here we discuss emerging threats within the connected home, the challenges faced by consumers and CSPs, and the opportunities that technologies such as containerization and virtualization can provide when it comes to security and IoT.



# “Everything is financially motivated. It’s all about money.”

**Q Why are cyber criminals targeting the connected home?**

**A** Everything is financially motivated. It’s all about money. So cyber criminals will go where the money is, and where the money is for them centers around volume and vulnerability. The Mirai botnet in 2016 was a game-changing moment, because it focused the attention of cyber criminals on the connected home.

Mirai used a brute force password attack. It would use different password combinations—such as ‘admin’, ‘password’, ‘password 1234’, things like that—and there were so many IoT devices that failed in that security model, that it spread like wildfire, ultimately affecting 10s of millions of devices around the world. So we went from a point in 2016, where we had a handful IoT vulnerabilities, to today, where we’re at over 5,000.

**Q What does 2023 look like, in relation to IoT threats in the connected home?**

**A** In some sense it will be business as usual, in that we expect the criminals to still target IoT devices, as they have had great success compromising many IoT devices to date, particularly routers, printers and IP-cameras. One evolution we have seen, and that I expect will grow, is the role of nation states looking to compromise IoT vulnerabilities. Already we’ve seen what we believe are attacks originating from Russia on routers, but industrial control systems and national infrastructure are also key targets.

**Q What are the key developments taking place in IoT right now?**

**A** In the world of the connected home, we see increasing opportunities for CSPs to provide better protection for home users

**Q Is it easy to tell if your IoT device has been compromised?**

**A** The only visible impacts that we’re aware of is you might see a slowdown on your Internet connection. That’s it. You wouldn’t see anything else. And partly that’s because of how hackers are using compromised devices, which is to pool them together to launch denial of service (DDoS) attacks and spam campaigns, which they can then monetize.

It’s all about scale. If cyber criminals can send out 10 million spam messages and get a 0.1% hit rate, that’s good enough. Elsewhere, a more recent area where we’re seeing IoT devices being used is in the mining of cryptocurrency. To crack the prime numbers involved in crypto mining you need lots of computing power. So, again, criminals are using the computing power of individual devices to form part of a bigger network.

# “There’s just no reason for a mail server to be baked into a fridge.”

and also add value to their core-connectivity offering, by adding home network protection.

At the same time there are some exciting developments taking place in the field of virtualization and containerization that will make it easier for operators to deploy third-party services, such as security into home gateways (routers). F-Secure is an active member of bodies such as the Broadband Forum and the PRPL foundation, which are creating an open, standards-based approach to delivering OTT (over-the-top) services that will significantly shorten time to market and improve lifecycle management.

### Q What are you main concerns about IoT?

**A** I have two concerns: security and privacy. I am a technophile, and as such I often have reservations about security models, so I will look at connected home products in a very detailed way. For example, I have a smart heating system, and I chose my vendor very carefully. And the driving force behind my choice of vendor was the security model.

My second concern is privacy, and this is why I don’t use smart speakers. This is because I’m very uncomfortable with the mass collection of data, and how they use it to create a mosaic of data about you. And in the last five or six years we’ve seen IoT goods come onto the market that break many security practices, because the company that’s created it doesn’t have a security background.

### Q Would standardization or legislation help?

**A** We don’t have a CE standard for security, and that could really help. Obviously, we have a CE standard for electrical items, which tells you that it’s been properly fire tested, power tested etc. But

# “A major issue is how long you’ll have certain devices for.”

when it comes to security, nobody’s got a clue, and it wouldn’t be that hard to implement, certainly in regulated markets like the European Union.

Also, in relation to Europe, EU legislation will come into effect at the start of 2024 which will require IoT manufacturers to improve the security in IoT devices, or they will not be able to legally sell in Europe. And it will be interesting to see how manufacturers will respond. I expect large corporations to react positively, but many smaller companies will struggle. At the same time, it will be interesting to see how the EU will be able to police this.

**Q Is it enough to tell consumers they are secure, or do you also need to show them?**

**A** We provide a visual overview for consumers, illustrating whether they’re protected, how many threats that might have been detected,  and that kind of thing.

And communicating this information is really important to people; giving them that sense of security. It’s fine telling someone they’re secure, but it’s really important to make it tangible.

**Q Are IoT devices particularly vulnerable to cyber attacks?**

**A** A major issue is how long you’ll have certain devices for. You will replace things like phones and laptops every couple of years, but you’ll have your fridge for a decade, possibly. And then you think about industrial goods, where these things are going to be on an even longer update cycle, of maybe 20-30 years. But what happens when support is withdrawn? Does that mean your smart fridge suddenly stops working? And those are very real risks. And then you have to consider the reason why that fridge is Internet connected in the first place. Samsung makes a fridge which effectively contains a mail server built into it. And there’s just no reason for a mail server to be baked into a fridge.

**Q How does F-Secure help protect devices in the home?**

**A** IoT threats are just one element of potential vulnerability that we cover with F-Secure Sense and Total.

The products we offer work together. Endpoint security is the most powerful protection you can have, purely because it’s working at an operating system level. It can interact directly with the operating system. But it has limitations, because there are devices where we can’t add security software at the operating system. And when it comes to connected devices, they’re usually Linux based. So F-Secure will never make antivirus software for your connected toaster or fridge. And that’s where the Sense product comes in. So it’s a symbiotic relationship between our products, which delivers the best protection.

**Q What future benefits might CSPs get from adding network security?**

**A** For security reasons, we need to see devices on a network, so we can apply the right security policies. And this could ultimately be a service in itself. Operators can derive benefit from it, because they can see what devices are connected, whether there are any issues (especially regarding Wi-Fi), and then diagnose them remotely. That’s very deep technology. And it could eventually help CSPs self-diagnose and self-heal, especially when it comes to Wi-Fi issues, before the customer even considers calling their helpdesk to make a complaint or raise a ticket. And these are areas where we’re working closely with partners, to open up new ways to add value.

# Cyber Security CSI: 5 top threats

We hear about the latest threats. But what do they actually look like? And how do they affect their victims? We reveal all.

A cyber crime scene could be anywhere. It could be on the desk in a child's room. Or on a laptop trying to get free airport Wi-Fi in Prague. It could even be sitting in your pocket, and you may not know that for days, weeks or months.

Unfortunately, too many of us will be victimized by cyber criminals. Nearly one in three internet users say they've dealt with cyber crime in the last 12 months, according to a recent F-Secure survey.* The data shows that the more active you are online, the more likely you are to be a victim. One in ten report that they have been hit by malware or a virus or premium SMS scams, while about one in 20 say they've dealt with an email hack, unauthorized access to their social media accounts, or credit card fraud.

The effects of cyber crime range from emotional distress to financial losses. More than six in ten victims of cyber crime (62%) say they experienced stress. A majority (51%) say the crime robbed them of time. And more than two in ten (22%) say that they experienced the loss of actual money.

Cyber Security CSI aims to reveal how common cyber attacks—infostealers, phishing, spam, bad Android apps and scams—look as they're unfolding. The goal is to help you to avoid any serious losses by identifying these cyber crimes, ideally as they're in progress.

Using an internet security solution, like F-Secure Total, will ensure that you'll avoid just about all these threats. But no software can yet prevent all human error. Only preparation and education can guide us to better decisions. So, some insight into how these threats unfold may help keep your device from turning into a crime scene. Let's dig in.

* F-Secure Consumer Survey, December 2022, n=4000, 'Simply Protected'

1

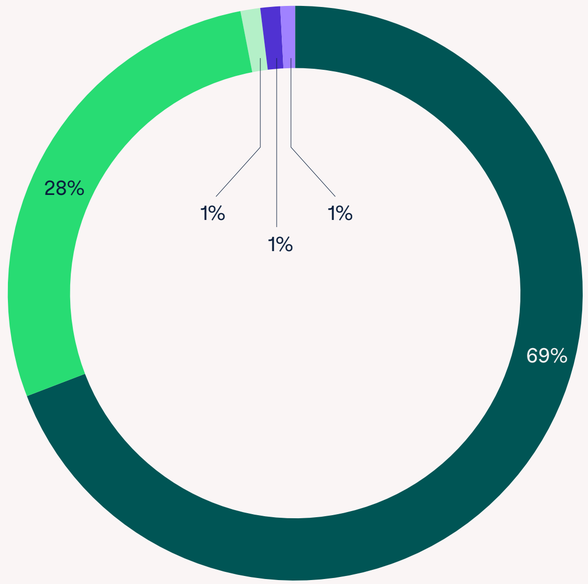
# Infostealers

Information stealers, or infostealers, have become far and away the most common type of malware faced by anyone running Microsoft Windows PC. They suck up hundreds of thousands, if not millions, of credentials, every month.

Nearly seven out of ten (69%) of the threats observed on Windows in 2022 were infostealers. Since the beginning of this decade, the rise of infostealers has become impossible to ignore, and increasingly, the data this threat steals can be used to defeat multi-factor authentication, including cookies and system data.

## What is an infostealer?

Infostealers fit the definition of a trojan, malware designed to mislead users by posing




## Windows threats during 2022

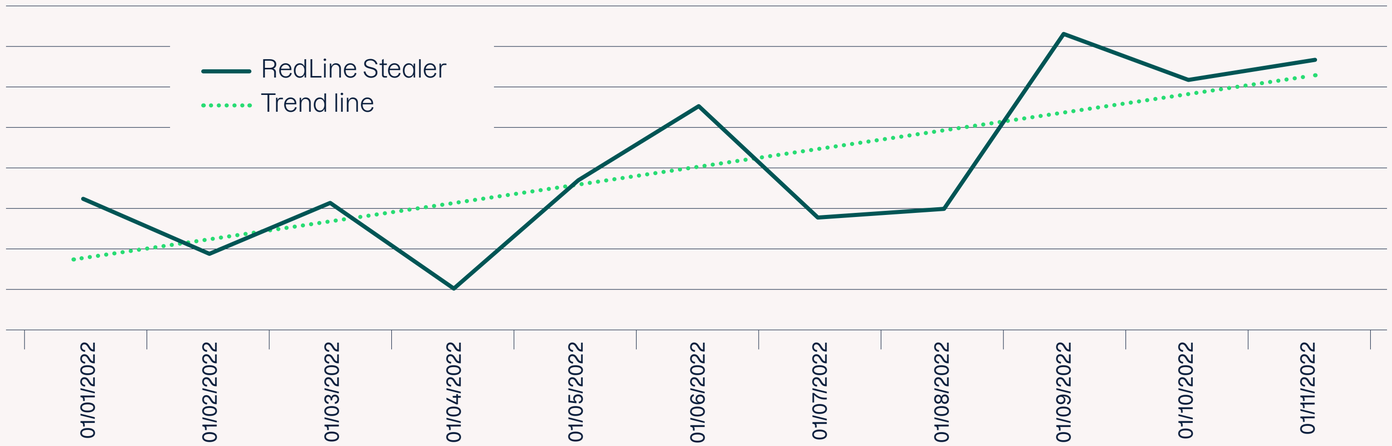
In 2022, consumers faced infostealers and similar threats that silently steal users' information far more than any other. Downloader Trojans that lead to malware to be downloaded from external sources made up about one out of four infections (28%). Ransomware, Banking Trojans, and CoinMiner trailed while still racking up significant infections.

Infostealer
Downloader Trojan
Ransomware
Banking Trojan
CoinMiner

Source: F-Secure monitoring of prevalent threats.

## How RedLine Stealer spread during 2022

The infostealer known as RedLine trended up throughout 2022 with the infections racking up millions of stolen credentials.




Source: F-Secure telemetry tracking high-level visibility of infection hits.

as legitimate software. Once a user has been tricked into installing an infostealer, it will run silently sucking up targeted data—including credentials stored on the browser, logs of instant messaging clients, and much more. Other variants of information stealer can capture screenshots, track keystrokes, and help criminals loot cryptocurrency wallets.

### How to avoid infostealers

Utilize automated antivirus scans from an internet security solution, like F-Secure Total, on a regular basis. If an infection is found, change any passwords that may be stored in your browser, along with the login and password credentials for any services you've accessed through your PC. Always monitor your online identity using quality identity theft prevention like F-Secure ID Protection, which is included in F-Secure Total.

## RedLine Stealer distribution timeline for 2022

An overview of how RedLine Stealer spread during 2022

| | | | |
|---|---|---|---|
| January 2022 | Fake Omicron stat counter | Malvertising/ Rig Exploit Kit | |
| February 2022 | Fake Windows 11 upgrade installers | | |
| March 2022 | Fake Valorant cheats on YouTube | | |
| April 2022 | Rig Exploit Kit | | |
| May 2022 | Fake bot for Binance NFT Mystery Boxes on YouTube | | |
| August 2022 | Fake 'Cthulhu World' play-to-earn | Fake shareware sites | |
| September 2022 | Links from 2K Games' hacked help desk | YouTube gaming videos | Google Search: 'Photoshop crack keygen' |
| October 2022 | Discord via PDF Links | | |
| November 2022 | Fake MSI Afterburner (Windows gamers) | | |

Note: Actual samples on the campaigns may have been in the wild earlier than publication.

## HOW THEY WORK


**1** Criminals' ability to profit off infostealers begins and ends on the dark web, where various versions of the threat are sold.


**2** Criminals establish an alluring method designed to make victims click. An unwitting victim initiates the download. Once installed on the victim's PC, the stealer collects the targeted information and awaits further instructions from the criminals.


**3** The stolen credentials are packaged with other victims' data to be sold on the dark web.

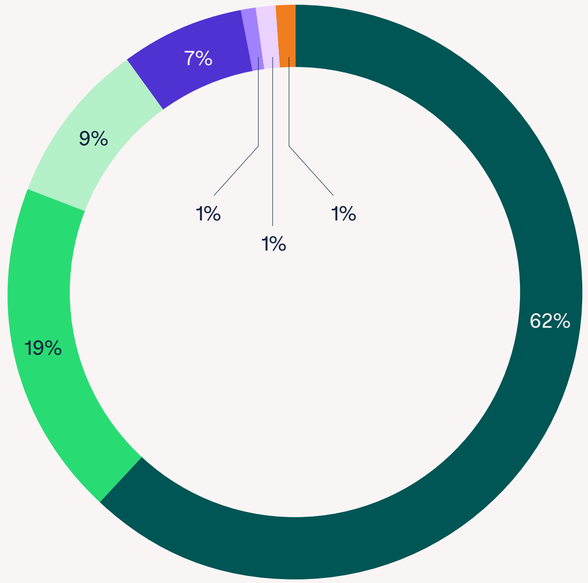
1. RedLine Stealer Advertisement (Source: cyberint.com)
2. Fake Windows upgrade website (Source: threatresearch)
3. Logs containing stolen data from RedLine victims (Source: socradar.io)

# 2

# Phishing

Phishing remains a threat nearly everyone on the internet must face. This is because the tactic works, especially when targeted at vast numbers of potential victims. Phishing's continuing effectiveness comes from criminals adapting their techniques to target any platform or service that large numbers of users embrace. There's also an ecosystem that enables these attacks by providing relevant tools and targets that criminals can find, either through the dark web or on legitimate platforms like GitHub.

Threat actors usually target victims' banking and credit card information, with streaming services, social networks, and gaming sites being popular targets for phishers. As these platforms can contain credit card information or digital items, such

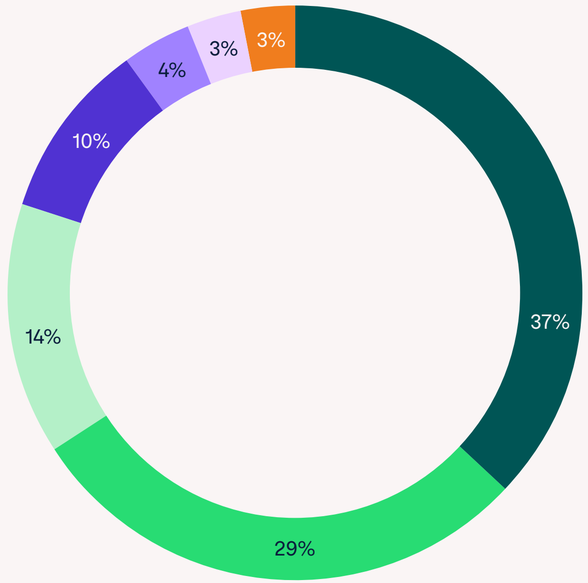



## Most imitated social networking platforms for phishing in 2022

Criminals love to use Meta's Facebook, the world's largest social network, as a lure for phishing attacks. Meta's other apps, WhatsApp and Instagram, come in a distant second and third as the networks most likely to be imitated. LinkedIn barely makes the top 20 of social networks by size but ranks fourth as a phishing lure.

Facebook, Inc. · WhatsApp · Instagram · LinkedIn Corporation · VKontakte · Naver · Others

Source: F-Secure Threat Intelligence.




## Most imitated gaming platforms for phishing in 2022

Phishing scams have become increasingly effective at targeting the billions of gamers around the world. Phony emails attributed to Steam, the biggest desktop gaming platform, make up the most common attacks. Scams posing as coming from Roblox, a gaming platform extraordinarily popular among internet users under the age of 16, rank second, followed by Garena, a free gaming platform based in Singapore.

Steam · Roblox · Garena · Mobile Legends · Axie Infinity · G22 Online Gaming · Others

Source: F-Secure Threat Intelligence.

as in-game currency, that can be sold on the dark web.

### What is phishing?

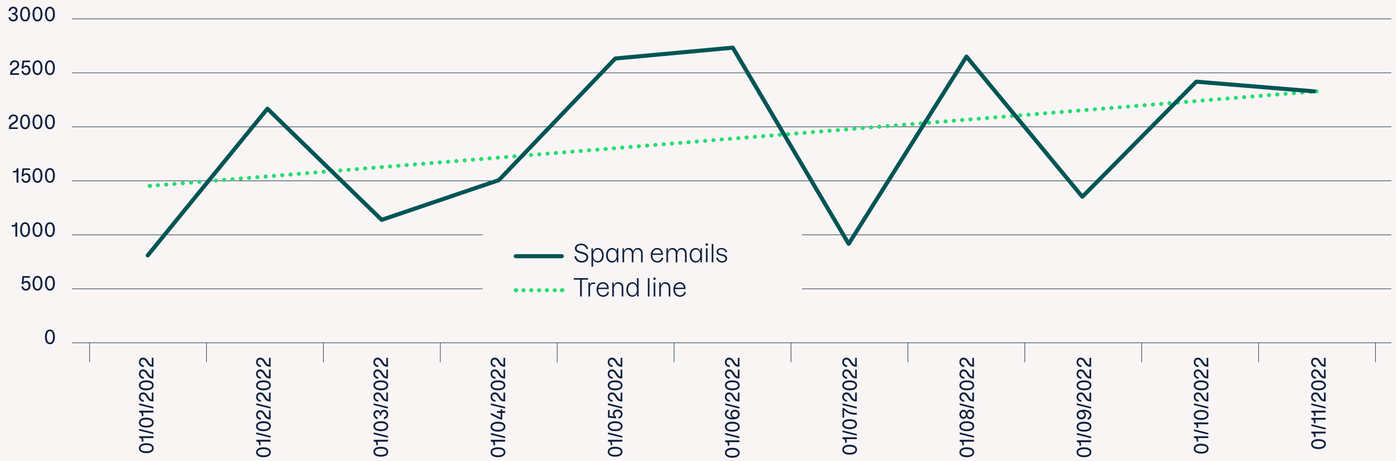
Phishing describes attacks that trick users out of private information or convince them to click on links or attachments that lead to malware. The attacks take place anywhere people receive communication including email, SMS, direct messages, or notifications. These attacks rely on different tactics to build trust with victims, which lure them into handing out sensitive information and money or clicking on a bad link.

### What to do

Change any phished password, along with any similar passwords. And if you've entered credit card details or financial information, cancel the card or set up a fraud alert on the account. Unfortunately, you may not know if you've fallen for a phishing scam, so use a service like F-Secure ID Protection in F-Secure Total, to monitor your data on the dark web.

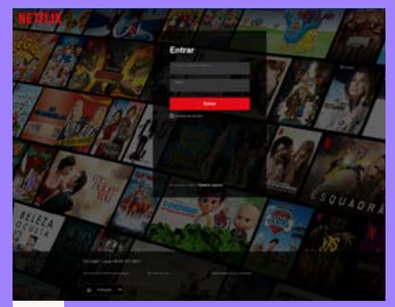
## Frequency of phishing emails imitating Netflix

Criminals spent 2022 exploiting the popularity of Netflix, the world's largest streaming service, for phishing emails. The trend line up suggests these attacks were effective as they increased throughout the year.



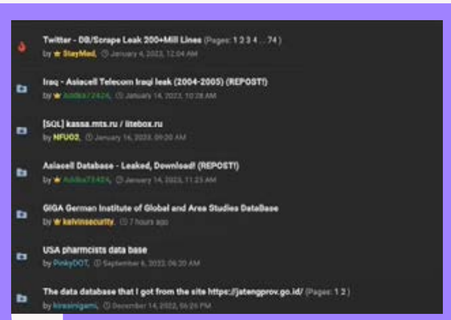

Source: Monthly spam volume based on F-Secure spam traps.

## HOW IT WORKS




**1** Using a wide variety of tools, criminals establish an extremely realistic looking phishing site.

Source: Alexandre Siviero.




**2** Criminals purchase breached, leaked, or scraped data. Using some pretense that requires the recipient to offer private data, criminals approach the victims, usually through email or SMS.


**3** After entering data into the phishing site, the victim is then redirected to the real version of the site to camouflage the scam. The criminals collect the data in the command-and-control channel of their choice.

3

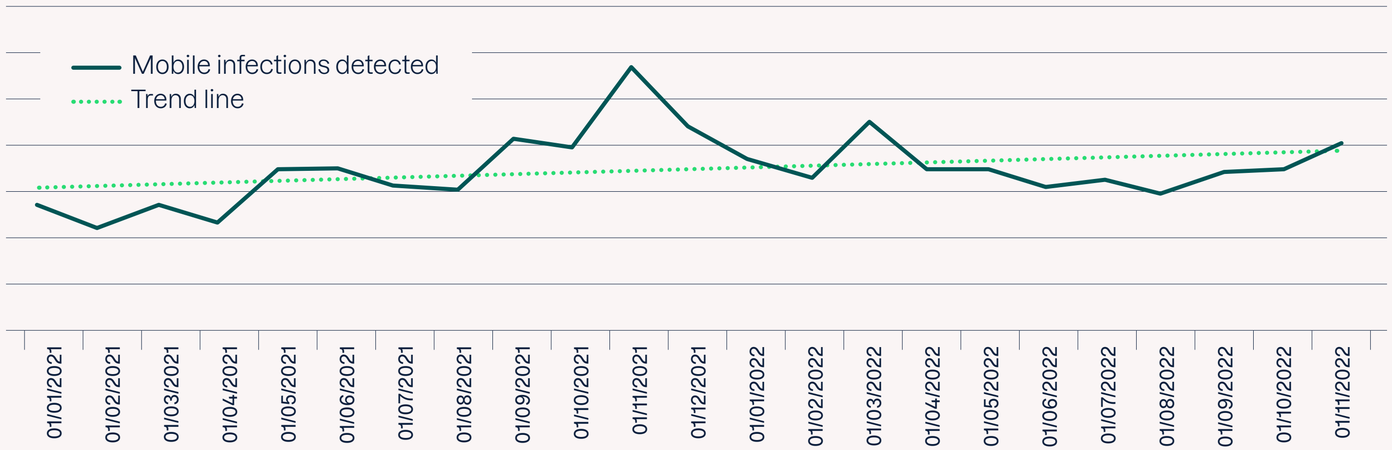
# Bad Android apps

Infections targeting Android devices increased between 2021 and 2022. More than half of these threats come from a category of bad apps known as PUA (potentially unwanted apps), followed by malware, which make up nearly one-third (32%) of all mobile infections.

The top Android infection overall falls under the category privacy risk tool apps. Most examples of this infection are unofficial builds of WhatsApp, which function like the official version while offering additional features, such as more themes and emojis. These apps were mostly not malicious, but they may include unwanted tracking and even malicious modules. In 2022, Triada—a trojan that has been targeting Android devices since at least 2016—was found inside these

## Mobile threat infections over 24 months

When it comes to mobile malware, Android remains the most popular target for criminals. In 2022, the number of infections targeting devices running Google's mobile operating system trended up slightly as the year progressed.




Source: F-Secure infection hits.

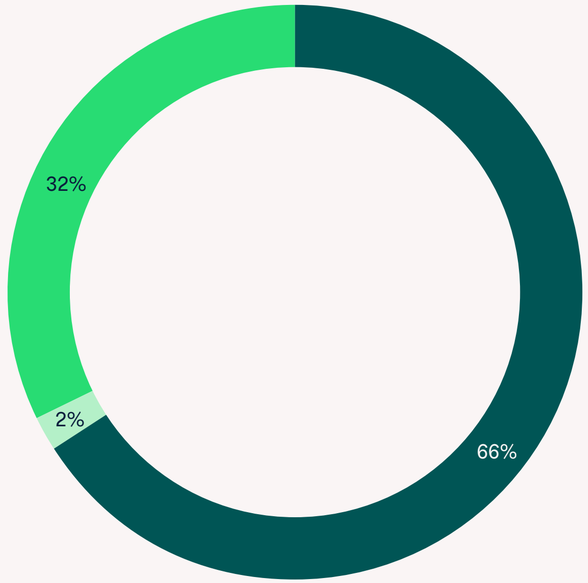
unofficial builds, using these bad apps as a launching point for more attacks.

### What is a bad app?

The line between potentially unwanted apps and malware can be blurry. However, malicious apps cross the line by taking over users' accounts. Actual Android malware includes banking trojans, such as SharkBot, which steals credentials. Typically, these threats are found on third-party marketplaces or other sites outside of the Google Play Store. But recently, threats including SharkBot have appeared in the official Play Store.

### What to do if you suspect foul play

If you think an app is tracking you or contains malware, delete it—especially if it didn't come via the official store. To do this, open Settings in Android. Choose 'Apps & notifications' and 'See all apps'. Select what to uninstall and follow the instructions. If it doesn't work, hold 'Power Off' for a few seconds to restart in 'Safe Mode', and then try again.




## Mobile threat type distribution

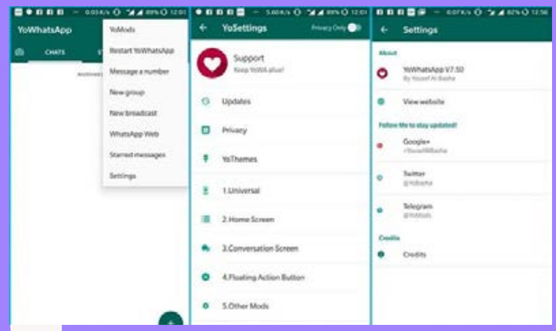
Potentially unwanted apps, which include monitoring software that can be installed without the user's knowledge, constitute the majority of mobile threats detected. However, nearly one out of three mobile threats detected (32%) can be clearly defined as malware that aims to steal private data. Files that test device security make up a small but noticeable slice of the threats observed.

- Potentially unwanted apps
- Malware
- Other

Source: F-Secure infection hits.

## HOW THEY WORK


**1** Inside SnapTube, a popular free Android video downloading app, a user sees an ad for YoWhatsApp, an unofficial version of WhatsApp.




**2** Once installed app functions just like the official WhatsApp. Unfortunately, the installation also grants the Triada trojan the same permissions as the app. Criminals can now upgrade users to premium subscriptions without the users' permission. And their WhatsApp accounts are at risk of being hijacked and used for carrying out other attacks.

4

# Spam

Spam has become an annoyance that generally gets buried in the junk folder of our email boxes, as both the filters and laws attempting to reduce this scourge have improved. Still billions of pieces of spam are sent out every day, and it remains a tool criminals utilize to spread both scams and malware.

‘Free Gift’ scams delivered through spam proved to be popular throughout 2022. These scams weaponize names of popular brands, including Amazon, Apple, McDonald’s, Costco, and major airlines. They lure users to a website with the promise of free ‘gift cards’ and other prizes. All the victims must do is answer a survey and offer information, which may include personal data and credit card information. The data stolen is then used by

criminals for financial gain, which includes fraud and identity theft.

### What is spam

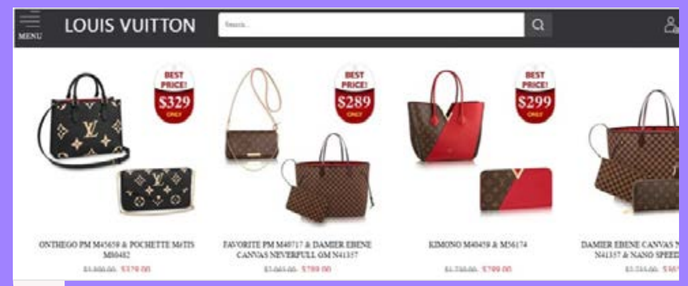
Spam is any unwanted, unsolicited bulk digital communication—including email, messages, and social media posts. The goal of spam is generally financial gain; tactics range from attempts to sell products or services to mass cyber crime campaigns spreading phishing scams or malware.

### What to do if hit by spam scammers

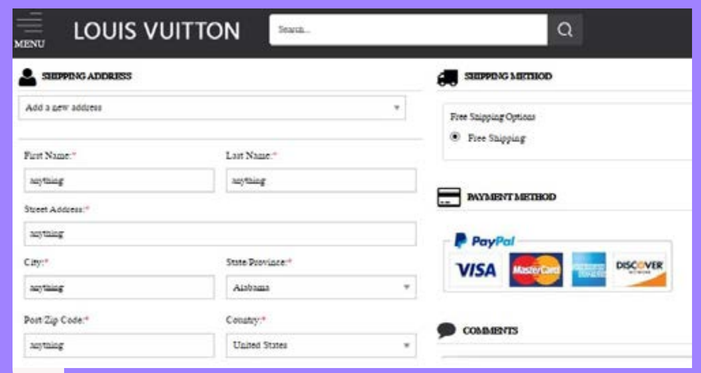
Stop any transaction as soon as you feel it's suspicious. If you've already made a payment, contact the provider that carried out the transaction—in this case PayPal—to cancel or contest the payment. Credit card companies make it relatively easy to reverse payments, which is a good reason to use credit cards for all online payments. Internet security that includes Browsing Protection, like F-Secure Total, will save you from scams by blocking malicious sites.

## HOW IT WORKS


1 The victim receives a solicitation that offers a luxury bag at an unbelievable price.




2 The link leads to a bogus yet convincing website with more incredible offers.




3 For the shipping address, any text works in all the fields.


5 After sending a payment to someone named 'James', the victim receives nothing.


4 The scam then guides victims to select 'For friends and family'. Notably, PayPal's fraud protection does not cover personal payments.

5

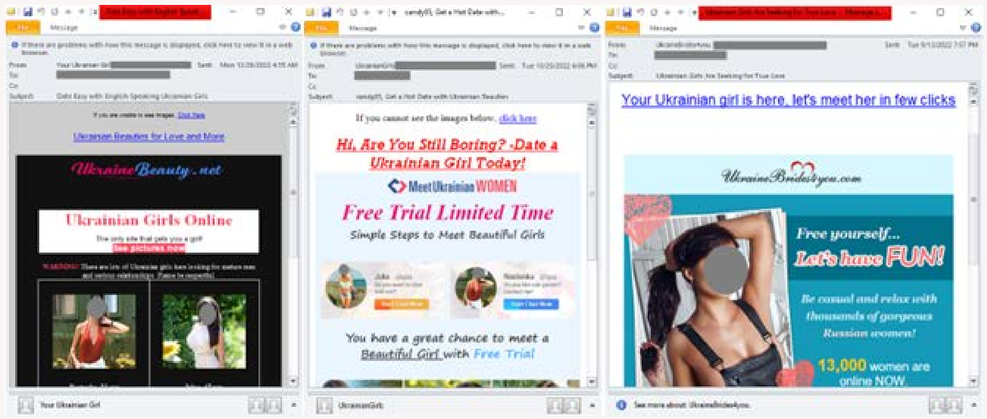
# Scams

Scams are not unique to the internet, but the internet is uniquely useful to scammers, who can target victims anywhere. Using social engineering that encourages victims to believe wishes can come true, scammers provoke irrational behavior. Even the best internet security in the world cannot prevent you from sending money to a stranger you met online, if you believe doing so is in your best interests.

Scammers are ruthless in their willingness to use anything to manipulate victims. Throughout 2022, criminals exploited the invasion of Ukraine for numerous of scams, often exploiting the worst miseries of the war.

## What is a scam

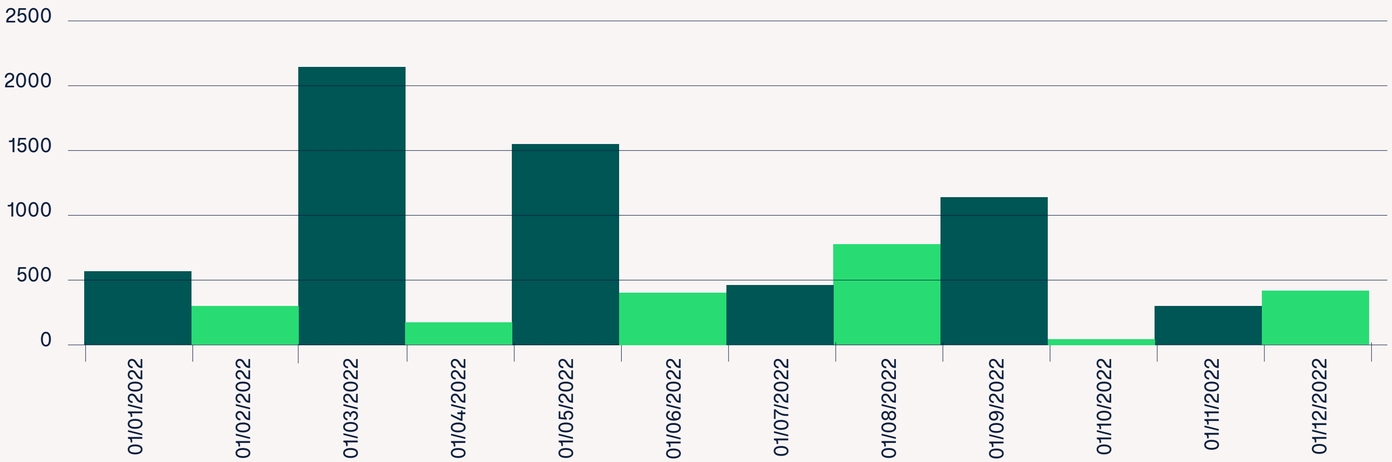
The US Federal Trade Commission (FTC) tracks reports from victims around the world.




These examples illustrate how awful typography can be a sign of cyber scams.

## Email scams exploiting the Ukraine crisis

Attempts to commit fraud using scams related to Ukraine spiked immediately following the invasion of the country by Russian forces. Since March 2022, these scams have varied up and down as the year progressed, but continue to be quite common.




Source: Monthly spam volume based on F-Secure spam traps.

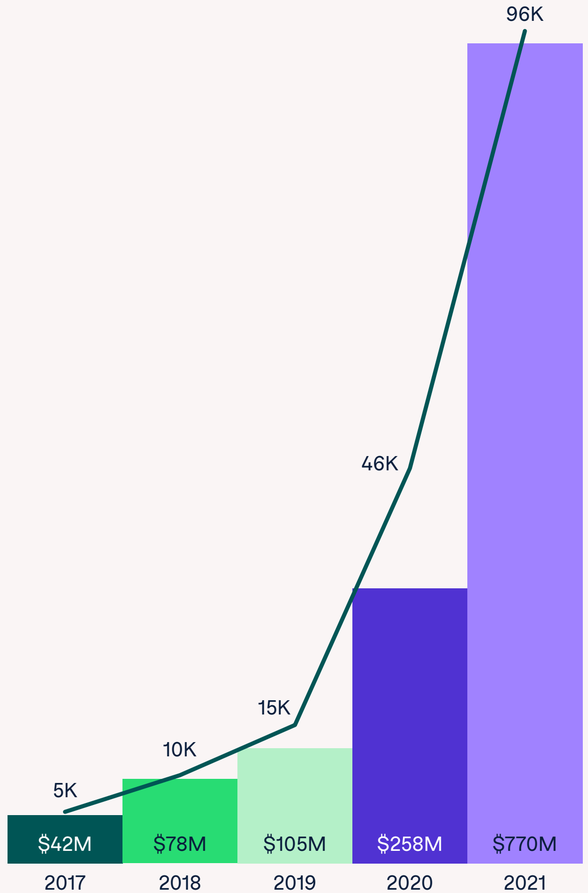
The most prevalent scams fall into the categories of online shopping, investment, business impostors, vacation and travel, and romance. And the emergence of cryptocurrency, which is far more difficult to track than traditional financial transactions, has driven online scams to new levels.

### What to do if you fall for a scam

Contact law enforcement (if safe to do so) and any bank, wire transfer company, or credit card provider used to send the scammer money as soon as possible, no matter how embarrassed you may be. If you sent cryptocurrency, reversing the payment may not be possible. Still, you should report the fraud to the company you used for the transaction. You should also monitor your identity using a service like F-Secure ID Protection, which is included in F-Secure Total.

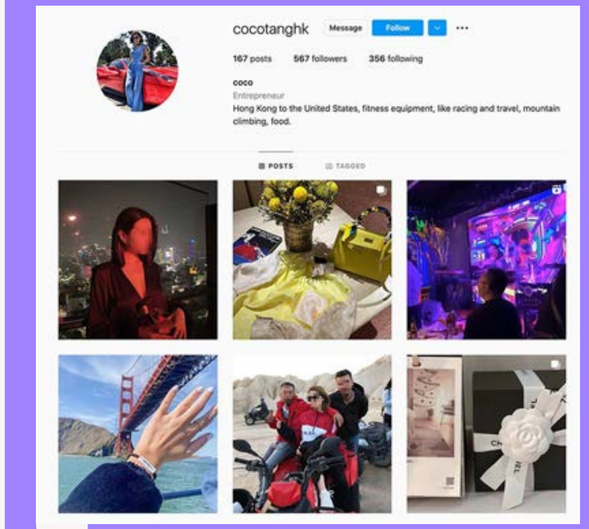
## Fraud increase since 2017

Reports about fraud originating on social media soared over five years. 2021 total reported losses were about 18 times what they were in 2017, and the number of people who reported losing money in 2021 grew to 19 times higher than those reports in 2017.



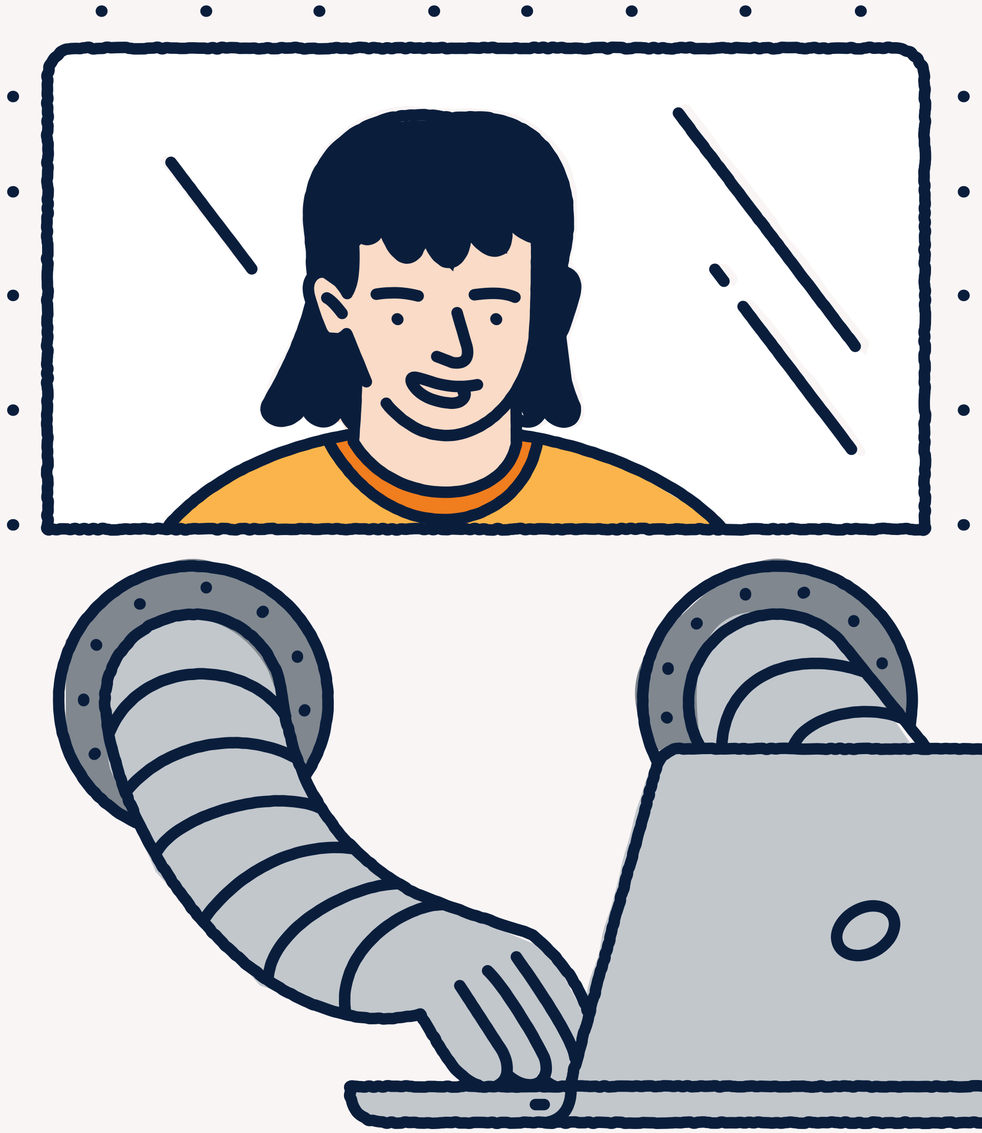

Figures based on fraud reports sent directly to the FTC, indicating a monetary loss and identifying social media as the method of contact.

## HOW THEY WORK




**1** ‘Pig butchering’ scams begin with a convincing, alluring false identity. The scam gets its name from the practice of fattening a pig before slaughter.


**2** The scammer approaches, often by pretending to mistake the victim for an old friend. Gradually, the topic of investments comes up. The scammer then convinces the victim to get the app MetaTrader and put money in a ‘brokerage’ account.



# Master your passwords

Every month millions of people have their passwords stolen. Here we explain how to keep your passwords secure.

On a weekly basis you're likely using around 10 different accounts, but did you know that on average each of us already has close to 100 online accounts? Most of us can't even name all sites we've been creating accounts for – think about all webstores you've made a single purchase from, or perhaps those mobile apps that force an account creation in order to function. Now, if we don't even remember all the services we've signed up for, how could we remember all the required passwords?

## Multiple weak passwords

To solve this, people tend to do one or both of the following: they either reuse a handful of passwords (or just one) across all services, or they make some slight but obvious alteration to their common password (like 'P@sswordFB' for Facebook, 'P@sswordIG' for Instagram, and so forth), resulting in multiple weak passwords.

The issue with both is the same: credential stuffing. In a nutshell, it's likely that your login details have leaked through at least one data breach, and now criminals are trying that one leaked email address + password combination to access a wide range of online services. So, as the name implies, they're 'stuffing' your credentials in many different locks, and hoping that they open as many as possible. This is a very popular technique, because it simply works due to reused and weak passwords. By accessing just one of your passwords through a data breach, criminals can now take over several of your accounts. Similarly, if, for example, Facebook login credentials have been leaked, it doesn't take a criminal mastermind to look for all mentions of 'FB' in passwords, and automatically replace them

with 'IG', and then test those credentials in Instagram.

To combat the impossible task of remembering all passwords, many people have begun to store their credentials in their web browsers. In fact, in a recent survey 75% of respondents answered they save at least some of their passwords in their web browser. This is a step in the right direction, but, unfortunately, the cyber criminals have noticed this as well. In 2022, the 'infostealer' malware type gained popularity among cyber criminals, and it was often specifically used to steal login credentials stored in browsers. For example, in December 2022 alone, F-Secure saw 23 million credentials stolen with malware such as RedLine Stealer, Raccoon Stealer and Vidar Stealer.

## Password no-nos

Sometimes passphrases have been suggested as a replacement for traditional passwords. Often passphrases consist of 3-4 random words written together, forming a 'password' that's relatively easy to remember and almost always longer than its traditional counterparts. And when it comes to passwords, bigger is better. However, when there are hundreds of passphrases to memorize, the system becomes just as impossible for us humans to remember and keep track of.

Passphrases gained their 15 minutes of fame several years ago when a popular webcomic XKCD illustrated how the passphrase 'correct horse battery staple' is superior to the password 'Tr0ub4dor&3'. While this is technically correct, we're willing to bet that a lot of people started using 'correcthorsebatterystaple' as their password, which brings us into another big password no-no: common passwords. Using massive lists of common passwords, criminals try them one by one to gain access to accounts. This technique is referred to as 'dictionary attack', as it often can include a literal dictionary's worth of words that the automated attack goes through to see if one of them has been used as the password for the account the criminal is trying to access.

So, let's summarize: we all have a hundred or more online accounts. For each of them we should have a password that is strong, and—most importantly—unique, meaning we only use each password to log in to a single service. Some people even advise that: 'a good password is one you can't remember'. Which poses quite a conundrum.

However, modern problems require modern solutions, and this is where password managers come into play. A password manager is an application that not only generates strong and long passwords for you, but it also stores them securely. To access your vault of passwords, you only need to remember one 'master password'. This, of course, needs to be strong and unique as well, but we're all much better equipped to remember just one perfect password than a hundred or more of them. With F-Secure Total, your passwords are monitored, you will be alerted of breaches should they occur, and you can generate and manage strong passwords for every online account that you have.

**"And this is where password managers come into play."**

### EXPERT TIP

"Most online services nowadays offer two-factor authentication (2FA), which increases the security of your account. If the 2FA is available, do consider turning it on. With this extra layer of security, even if someone steals your password, they still only have half of the 'key' needed to get into your account."

**Sarogini Muniyandi,** Manager, Threat Protection Engineering

Two-factor authentication (2FA) works by adding an extra layer of security to online accounts beyond your username and password, requiring an extra login credential (such as a one-time passcode, sent to your phone via SMS). By utlizing two forms of identification, accessed via a third-party authenticator (TPA) or separate device, 99.9% of automated attacks are prevented (according 2019 research from Microsoft).

# 5 killer phishing scams

Phishing is one of the most profitable forms of activity for cyber criminals – and one of the biggest threats for online users. In this article we will look at examples of phishing from 2022.

**Phishing overview:**
Phishing refers to the act of tricking users into handing over personal details or money to criminals.
Phishing is used to steal login credentials and personal details, which the criminals can then use for account takeover and identity theft.

Criminals can also sell hijacked accounts, or their contents, use these accounts themselves, and force victims into paying the attacker. The end goal for criminals is predominantly to get money. The information stolen with phishing is just a means to an end.

1

# Social network account phishing

Based on our data (see page 15), Facebook, WhatsApp, Instagram, and LinkedIn were the top social media platforms targeted with phishing in 2022. Criminals were after social media credentials, personal information, and financial data.

**How to spot the attack:** Comes via friend request and messages from unknown profiles promoting links to web pages.

**How to avoid it:** Run safe browsing protection. Don't accept friend requests from unknown profiles. Set an alternative email or phone number for retrieving your account. Use unique passwords and two-factor authentication.

# Phishing in the name of Netflix

A brand you know gets your attention easier than an unknown one. That's why criminals mask their phishing to resemble well-known brands. In 2022, Netflix was one of the brands that were most used for email phishing campaigns worldwide (see page 16).

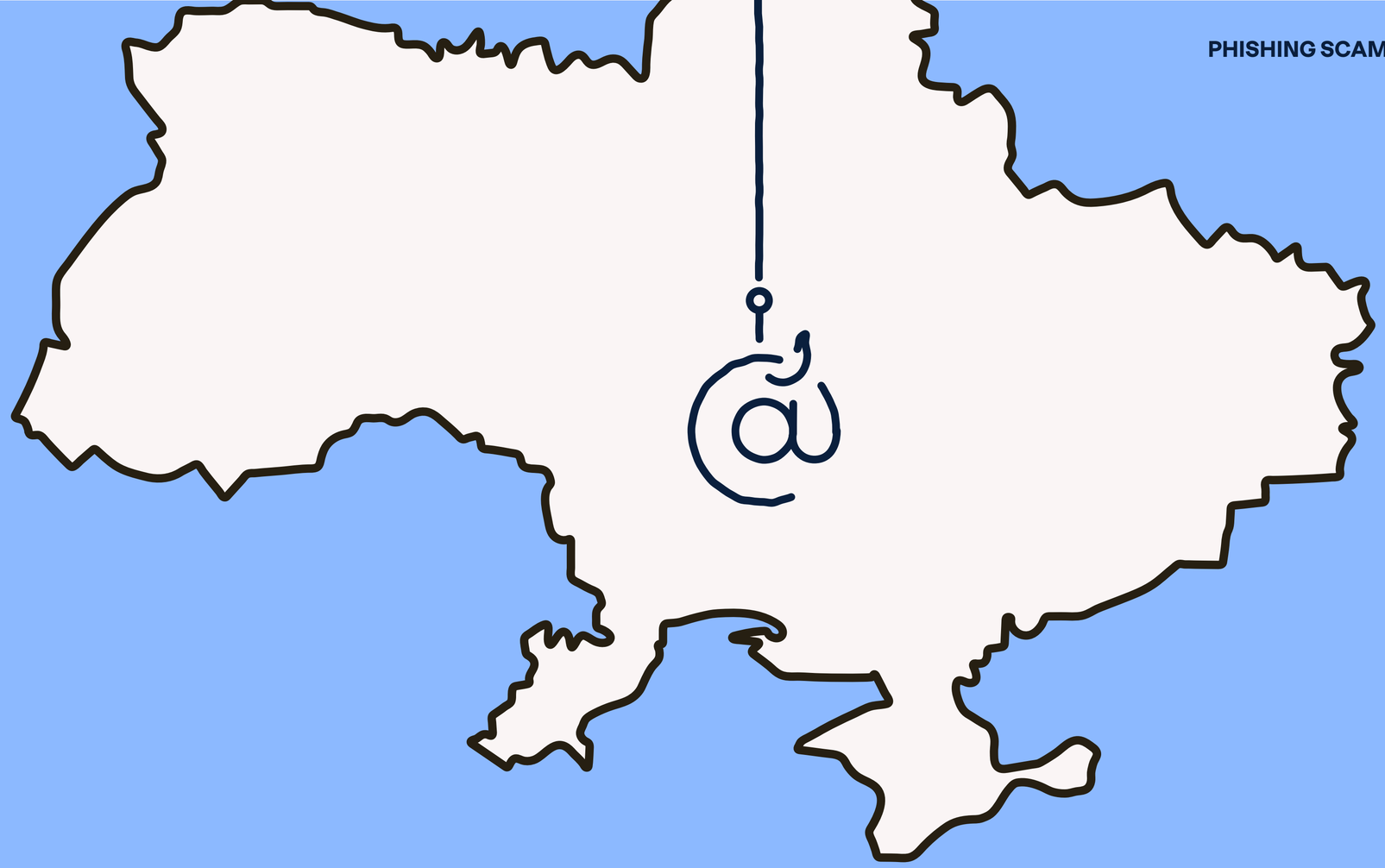
These emails told the receiver that their automatic payment was declined. To fix it, the victims were lured to update billing information through a link which led to a fake login page. Once the victim submitted their login details, the attackers were able to take over the account.


**How to spot the attack:** An email from Netflix with a "your payment was denied" message, and a link for fixing it. Inspect the sender field to spot typos and suspicious email addresses.

**How to avoid it:** Don't open the link. If you are unsure, sign into your account through an app or browser and check your payment status.

In the phishing message opposite, warning signs include suspicious sender info

# Contemporary topics: Ukraine



Phishing campaigns often utilize contemporary topics. It's easier to get attention when people are already interested in the topic. Therefore, the war in Ukraine was a major topic used in phishing in 2022 (see page 21).

Some of these campaigns preyed on people's will to help. This kind of phishing was spread via email and in the name of charity organizations, like the Red Cross. The victims were lured to "donate" cryptocurrency to help Ukrainians.

Many campaigns also lured victims to contact 'hot Ukrainian girls' looking for love. Believing they were conversing with Ukrainian women, the victims needed to create a paid profile on a dating platform. The victims regularly needed to pay more to keep on chatting or to unlock more photos.

**How to spot the attack:** Emails promoting help for Ukraine by paying in cryptocurrency. Alternatively, emails promoting paid dating sites with 'Hot Ukrainian girls'.

**How to avoid it:** Cryptocurrency payment is a red flag. Trust only well-known charities. Use payment information stated only in their website. People seeking real love will not contact you through paid dating sites.

4

# Smishing ‘Hi Mum’ scams

The ‘Hi Mum’ scam is an example of smishing (phishing involving phone messaging). The attack begins with a WhatsApp message from an unknown phone number, starting with the words ‘Hi Mum’ or ‘Hi Dad’. However, in these cases the sender is a scammer posing as the receivers’ adult child.

The scammer told the receiver that the child’s phone has broken down and that this is their new phone number. The attacker then asks for money to pay an urgent bill or to buy a new phone; they say they need money because they can’t access their bank without the old phone; or some other explanation.

It can be difficult for parents to think rationally when their child needs help. This is what the scammers were aiming for. And they succeed: many victims from the UK, Australia and New Zealand reported losing thousands of pounds or dollars to scammers.

**How to spot the attack:** Look out for WhatsApp or SMS messages from unknown numbers claiming to be family members.

**How to avoid it:** Call the old number or send them a message on social media to check if it’s real. Don’t send money to people contacting you from unknown numbers.


Examples of ‘Hi Mum’ messages

Source: www.dailymail.co.uk

# Gaming-related phishing scams

There are billions of gamers around the world, and billions of gaming accounts. In addition to personal details, these accounts include games and downloadable content, like skins, weapons, and other virtual items, which can be very valuable. This makes gamers a major target for criminals.

Based on our data (see page 15), Steam and Roblox were the top gaming platforms targeted by cybercriminals.

In 2022, attackers used a technique called 'voting scams' to steal Steam accounts. The attack starts in a Steam or a Discord channel with a message appearing to be from a friend asking the victim to follow a link to 'vote for their team' The link directs to a phishing page. Once they click on it, their Steam account goes to the attacker.

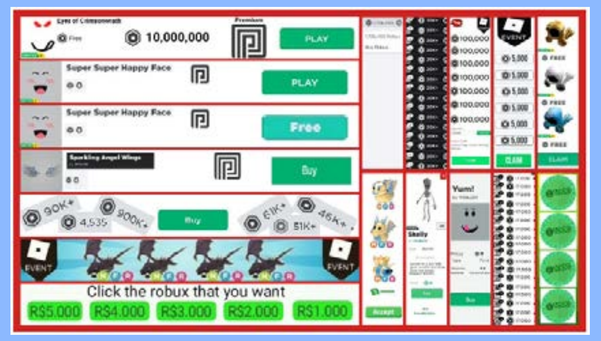
Another new technique discovered in 2022 is called a browser-in-the-browser attack. The technique uses a pop-up window within the browser to mimic a login website and to hijack Steam accounts.

In attacks targeting Roblox users, 'Free Robux' scams were popular. The attackers often used YouTube videos with a link to entice kids to get free Robux, the in-game currency used to buy items. Following the link led viewers to phishing sites where criminals collected login information that enabled them to take over users' accounts.

Phishers also hijacked Roblox accounts with fake User Ads, offering free items, Robux, Premium membership, or accessories. Clicking the ads led gamers to phishing pages where the users were asked to enter their username and password to claim the items.

**How to spot the attack:** Messages asking to vote for a team. Any unexpected message with a link is suspicious. Alternatively, ads or links promoting any free content that is normally paid.

**How to avoid it:** Run safe browsing protection. Don't enter your login details outside that particular service. Avoid free stuff, as it is often just a trick. Educate kids about phishing and scams.




Malicious Roblox ad used for phishing

Source: Roblox Forum

Laura Kankaala

**Threat Intelligence Lead** F-Secure

Laura Kankaala is Threat Intelligence Lead at F-Secure. Kankaala studied at Finland's Turku University of Applied Sciences before working as a security consultant for a number of companies including F-Secure. Kankaala is an active columnist, speaker, and podcaster, and she is a regular contributor to F-Alert, F-Secure's monthly threat report.

# How cyber security is getting personal

From stalkerware to shoulder surfing, F-Secure's **Laura Kankaala** reveals how relationship dynamics are shaping cyber security.

Picture a cyber criminal. Maybe an image of a person in black hoodie pops into your head. They are hacking into corporate systems or bank accounts of private individuals. That someone is a distant threat, taking advantage of flaws in systems and human nature for their profit. But what if the criminal is someone different? Someone closer to home?

## Complex relationship dynamics

Modern technology does not necessarily create new problems, but it extrapolates existing ones. Bullying has taken a foothold in online spaces from the Internet's very beginnings, only getting worse as the usage of social media made online social interactions more mainstream.

And you don't even have to be a celebrity to be publicly shamed on TikTok for something you've said or done. It doesn't even matter if your actions are taken out of context.

Complex relationship dynamics now exist online. Not only friendships, but even finding a partner now happens via apps. And the internet plays an increasingly more important role in cultivating romantic long or short distance relationships between people—sometimes between people who have never met in real life.

In these examples, we are exposing ourselves to new kinds of tracking and privacy related concerns, that do not only stem from the imaginary black-hoodie criminal mindset. We are subject to online stalking and unsolicited messaging. Our intimate messages or pictures may be screenshotted and used against us. Someone may even read our private conversations without our permission.

And our personal digital space can be invaded with little to no technical expertise. With 'Shoulder surfing'—i.e. stealing someone's passcode by discreetly observing them while they unlock their phone—being an ever-present threat.

## The persistent threat of stalkerware

Of course, there is technology that is made for, or at least can be utilized for stalking or violating someone's privacy. An example of such technology is 'stalkerware'—an app or software that can be installed on someone's device, which then grants wide access to it, including photos, messages, location and so forth. Installation and guidance of how to

use stalkerware is typically well documented, so it really doesn't take a Hollywood hacker to be able to use one against us.

Android devices are the easiest ones to monitor, with different types of stalkerware apps available, due to the way its permission model is designed. Upon installation, the perpetrator can choose to give very large privileges for the app, meaning they can constantly track what's happening on the screen. And based on our detections at F-Secure, we can see that installation of different stalkerware app families are now a persistent threat.

One of the telltale signs of stalkerware app installation on your phone is that the battery seems to run out very fast and the phone feels warm. This is because the stalkerware apps are constantly keeping tabs on the location of the device, which consumes a lot of battery power. You can also check your phone with Android antivirus tools.

### Changing relationship dynamics

But, as I described above, usage of malicious software such as stalkerware is not always needed to violate our privacy. People and relationship dynamics change. And you may lose touch with someone you previously trusted.

Maybe you've shared a Netflix password with someone you used to date, and you happen to reuse the same password in Instagram. Or perhaps you've given access to your email account so someone can take care of handling some business for you.

In all fairness, though, you should not stop trusting people because things may turn sour at some point in the future. At the same time, you should only do what feels right, and not share information or pictures that make you feel uncomfortable. And you should practice a sufficient level of security to protect yourself—use unique and strong passwords; change your device passcode, in case an untrusted partner knows it; and avoid sharing passwords.

Conventionally, information security—or cyber security—is mostly used in reference to defending people or organizations from crime. But when much our lives are spent online, the need for 'cyber security' becomes nuanced, and is more than just a means of keeping us safe from online burglars. In the end, we all need cyber security in our lives. Because it's not just about avoiding the criminal hackers, it's about being digitally independent.

**"Stalkerware apps are constantly keeping tabs on the location of the device."**

# 12 trends and predictions for 2023

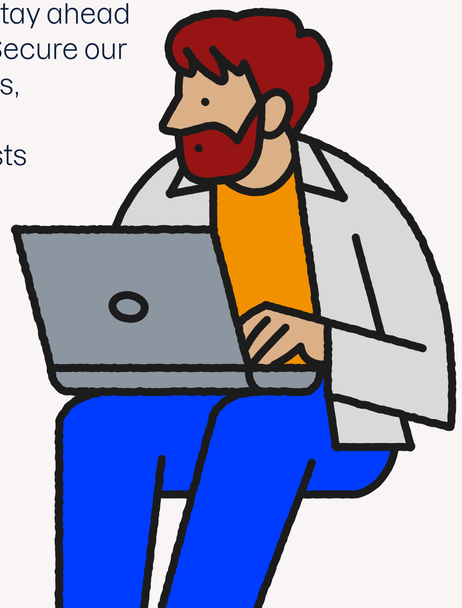
In this special report, leading experts within F-Secure share their cyber security trends and predictions.

Cyber security is a game of cat and mouse. Every year the threat landscape evolves, based on numerous factors, such as the increasing use of different devices and changing social behavior, like the increase in people working from home. And 2023 will be no different.

Phishing and smishing scams will continue to evolve. In a survey of 4,000 respondents (aged over 25 years) at the end of 2022, F-Secure found that 31% of consumers had been affected by cyber crime in 2022. In the same survey, 43% of respondents said that they had received phishing or smishing messages impersonating their bank or insurance company over the last 12 months.

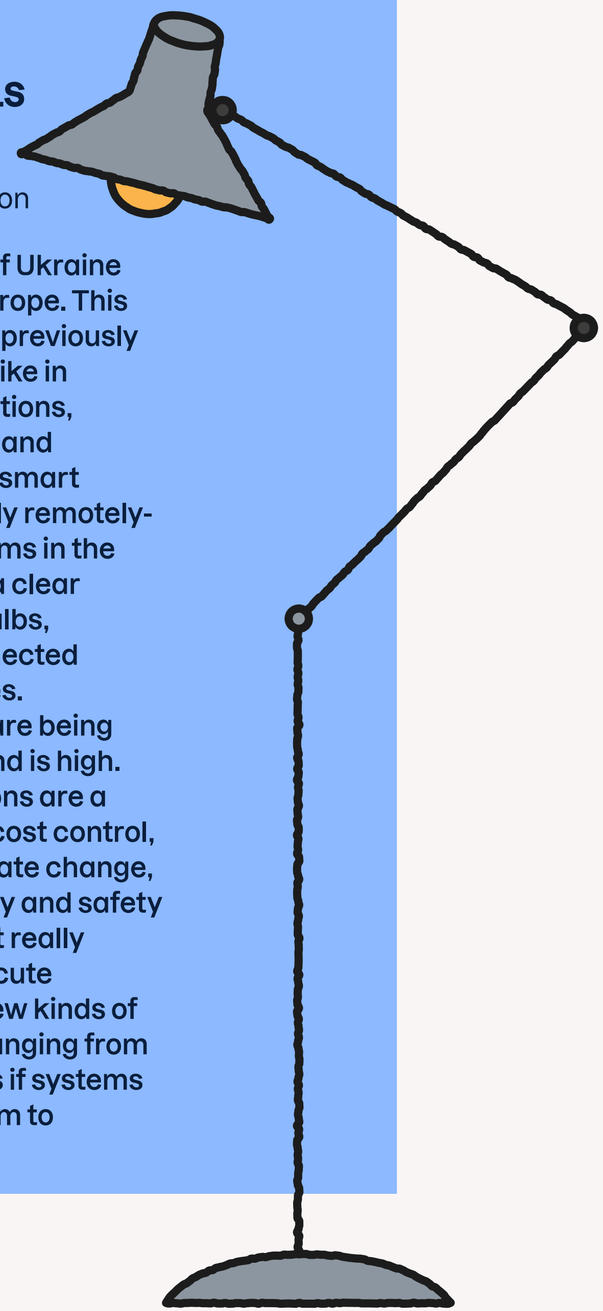
And with more than 20 connected devices in the average home (22 per US residence in 2022, according to Deloitte), and home-based working driving a need for stronger security, as employees access more sentitive data from home, the threats we face will continue to evolve.

Put simply, it's hard stay ahead of the curve. But at F-Secure our team of threat advisors, researchers, product managers, and analysts tracks the latest trends and emerging threats, enabling you to stay once step ahead of cyber criminals. And here they reveal their predictions for 2023 and beyond.



## 1 CONSUMER IOT ENTERING KILOWATT LEVELS

Mika Lehtinen
Research Collaboration



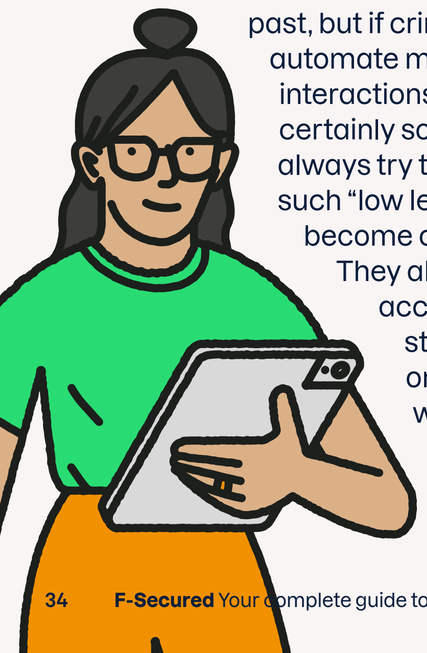
**The Russian military invasion of Ukraine triggered an energy crisis in Europe. This has made energy prices reach previously unseen levels, and caused a spike in demand for smart heating solutions, enabling consumers to control and optimize their energy bills. The smart heating solutions are essentially remotely-controlled, consumer IoT systems in the kilowatts power range. This is a clear upward shift from the smart bulbs, cameras and other small, connected devices popular in smart homes. Commercial energy solutions are being rushed to the market as demand is high. And while smart energy solutions are a very positive development for cost control, not to mention countering climate change, it is likely that the cyber security and safety aspects of the solutions are not really considered when solving the acute problem at hand. This opens new kinds of risk for the connected home, ranging from electrical safety to fire hazards if systems are compromised, causing them to malfunction.**

## 2 ACCOUNT TAKEOVER ATTACKS SCALE, MAKING EVERYONE A TARGET

Joel Latto
Threat Advisor

It's not out of the realm of possibility that we'll see criminals taking the same extortion pattern that has been used with ransomware, adapting it to account takeovers. After gaining access to your account (e.g., your social media profile, email inbox, cloud storage, etc.), bad actors could then sell you the "service" of getting it back. Alternatively, if users refused to pay, they might then proceed to publish your private information and delete your account.

This hasn't been viable in the past, but if criminals can automate most of these interactions (which is certainly something they always try to do), then scaling such "low level" crime might become commonplace. They already have access to billions of stolen login details on the dark web, which could be used in such attacks.



## 3 GAMERS WILL FACE INCREASING THREATS

Maria Patricia Revilla-Dacuno
Senior Threat Researcher

**Cyber criminals will continue to target information that can be used for financial gain. This can be in the form of more sophisticated infostealing trojans, or by targeting organizations. More cyber crimes will be coming as data breaches continue. Personal information, billing data, health records, or data of a sensitive nature has high value in the dark market. Attackers can use such data for taking over accounts, stealing money from bank accounts, and identity theft. And attackers can create fake profiles and commit more crimes such as scams and phishing.**

**Scam and phishing through email, text messages, social media and gaming platforms will continue, as these are channels that are part of consumers everyday life.**

**According to Statista, gaming accounts have the biggest share of market revenues in the consistent growth of global digital market—with an estimate of one billion online gamers worldwide. This number of users is projected to exceed 1.3 billion in the year 2025. With this growing number of users, we can expect that cyber criminals will continue to target these platforms for scams and phishing.**

## 4 TECHNO FUTURIST GRIFTERS

Fennel Aurora
Product Management
Community Lead

Many consumer software and device companies, along with uncritical media repeating their claims unchecked, have gone through multiple hype cycles for scammy technologies built on theft, mass harm, and human-rights violations, while never providing anything like what the techno futurists are promising. Examples include blockchain, metaverse, many different forms of luxury surveillance, and digital phrenology, and almost everything that is advertised as artificial intelligence, while being neither artificial nor intelligent (e.g. ChatGPT). These technologies, or at least the claims of these technologies, continue to be used as the smoke and mirrors in a vast array of scams and grifts, and this trend is accelerating. If companies and media tell you something is going to be the next big technology, magically solving everything, heavy skepticism is required. These claims have never been born out by reality, but the harms experts warn about from the start pollute our every digital moment.

## 5 PHISHING, SCAMMING, AND HOW AI CHANGES THE THREAT LANDSCAPE

Abdullah-Al Mazed
Senior Technical Product

You have probably seen some phishing email or SMS where you could instantly detect the attack, because of a grammatical or spelling mistake. Sadly, thanks to developments in the world of large language models (LLMs), those days will be a thing of the past. ChatGPT demonstrates how far natural language processing (NLP) has already gone, and how easy it is to write a very convincing mail or blog post with a simple prompt and a handful of keywords. Phishing attacks will only get more sophisticated with AI, and it will be an automated multi-step process, where the first communication will have no links to a phishing page, and no request to do anything specific, beyond initiating a conversation that will develop over time.

**"Phishing attacks will only get more sophisticated with AI."**

## 6 OLD SCAMS CONTINUE TO TARGET HUMAN VULNERABILITIES

Carl Blomqvist
Senior Technical Product Manager

Have you or your relative ever gotten a call from who claimed to be from Microsoft or Amazon? Although we get more knowledgeable and cautious about phone scammers, they can find us in the most susceptible, sensitive moments, and push on our guilt and humanity in order to steal money from us. Unfortunately, scammers' profits are still high.

Working in the area of cyber security we are used to devices and software having vulnerabilities. However, it is important to keep in mind that we humans have them as well. Criminals don't always use viruses or malicious applications. They can also use psychology and our good faith to harm us.

The good news is that F-Secure has users covered in their most vulnerable moments. We keep an eye on the various hazardous experiences that users may face, and find the techniques to prevent them, including protection against scammers.

## 7 DATA BREACHES CONTINUE, BUT VERIFYING AUTHENTICITY IS HARD

Calvin Gan
Senior Manager, Protection Strategy

Data breaches have been fueling headlines in 2022 and this will continue in 2023. Verifying the legitimacy and authenticity of these leaks will become harder, as information released is often saturated with data from the same database, sometimes packaged differently to gain hype, thus giving advantage to new threat actors, utilizing this information for short-lived extortion. The after effect of this could potentially be:

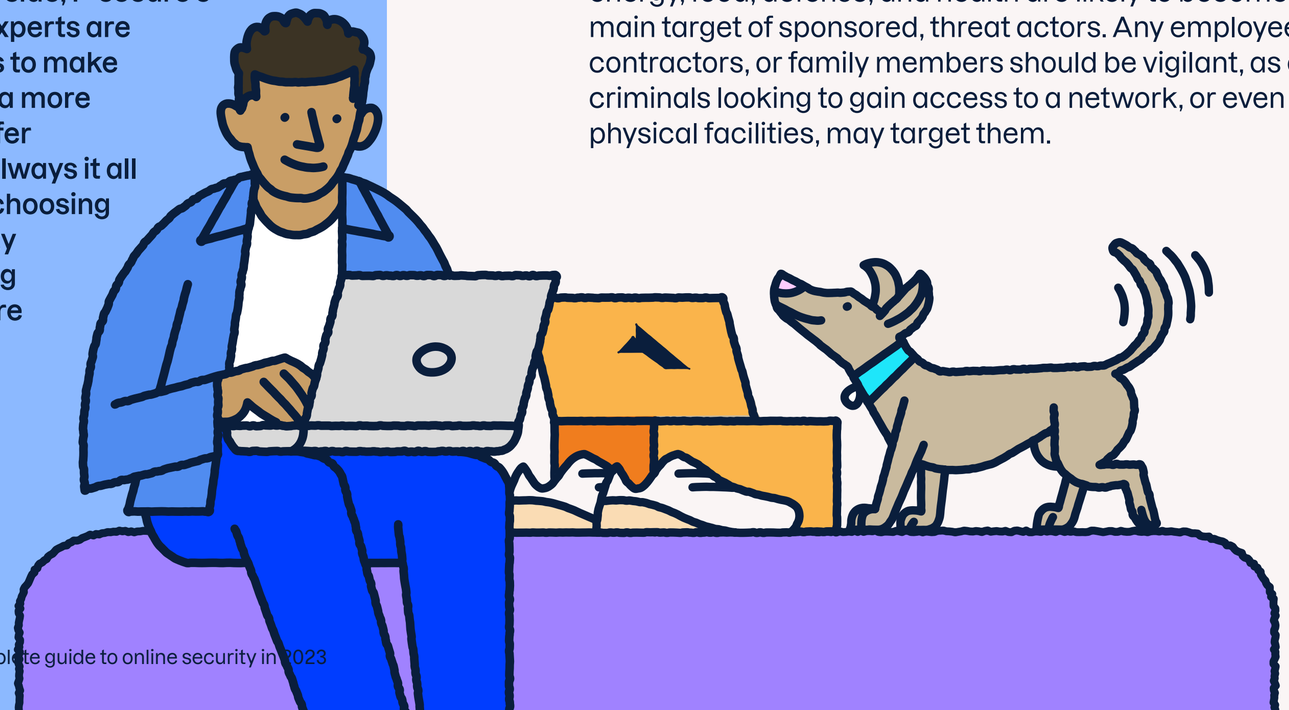
- Users receiving an increase of generic spam emails from threat actors trying to quickly capitalize on data leaks
- User fatigue in the wake of multiple breach notifications, where they may choose not to take any further action
- A rise of fake breach notification websites or services in an attempt for information harvesting or social engineering.

## 8 TRUST AND ONLINE SHOPPING

Ekaterina Makarova
Senior Quality Engineer

We need to be mindful while doing such basic things as online shopping. It has always been a minefield to differentiate between official websites that sell goods, and those who masquerade as official and trusted ecommerce operators. We cannot believe our eyes anymore, and online reviews can be easily contaminated. Criminals lure us onto websites that promise gold but give us financial loss or, even worse, ID theft.

On the positive side, F-secure's cyber security experts are working on ways to make online shopping a more pleasant and safer experience. As always it all comes down to choosing a trusted security product, enabling you to stay secure despite cyber criminals' persistence and creativity.



## 9 SPONSORED CYBERCRIMINALS TARGETING CRITICAL FACILITIES

Nadzreen Aqil Mohd Yusof
Junior Threat Researcher

The unstable political situation around the globe is expected to increase the number of sponsored cyber criminals—with strategic and specific goals—targeting critical facilities.

In 2010, Stuxnet highlighted the capability of cyber crime to damage a country's nuclear infrastructure, which ultimately costs money, time, and reputation. The use of technology in critical industries such as nuclear power provides sponsored cyber criminals with more possibilities to try to target a country's essential facilities.

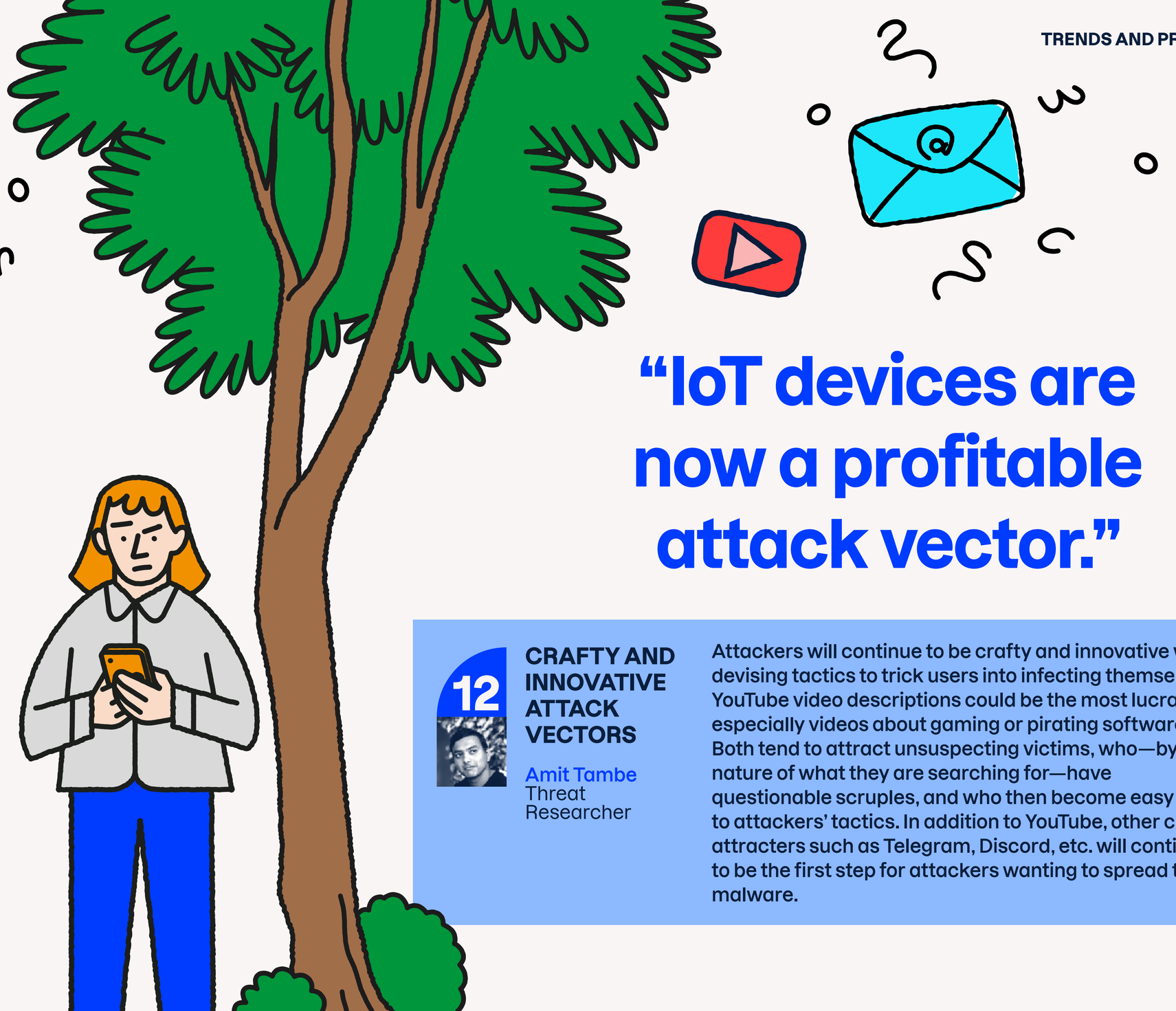
And companies linked to critical industries such as energy, food, defense, and health are likely to become the main target of sponsored, threat actors. Any employees, contractors, or family members should be vigilant, as cyber criminals looking to gain access to a network, or even physical facilities, may target them.

**"This opens the door for attackers."**

## 10 THREATS HIDING IN PLAIN SIGHT

Khalid Alnajjar
Threat Data Researcher

With the recent advances in machine learning, neural models can be compressed, shipped and executed on the client side (e.g., via a browser or mobile app). Malware and personalized phishing pages can be embedded in such neural models, where they would get activated only when a certain input is passed; otherwise, a legitimate output is returned. Additionally, neural models could learn to produce new variations of a given code while maintaining the functionalities. This opens the door for attackers to rapidly generate unseen attacks and camouflage them.



## 11 IOT DEVICES

Tom Gaffney
Director of Business Development, Network Services

Consumers are purchasing more and more IoT goods, with more innovation in this space than with traditional devices like mobiles, tablets and laptops. And global IoT devices are expected to grow to more than 29 billion by 2030, according to Statista. With this growing number, together with new IoT malware code publicly available, we can expect that more IoT threats will be developed.

As a relatively nascent market, many of the IoT goods we've seen developed miss security and privacy by design. This is improving with governments and agencies, such as the EU, driving a standards approach, but it will take years before security is commonplace. In the meantime, since the global attack by Mirai in 2016, cyber criminals have seen that IoT devices are now a profitable attack vector. And with IoT devices different security solutions are required to protect businesses and consumers.

**"IoT devices are now a profitable attack vector."**

## 12 CRAFTY AND INNOVATIVE ATTACK VECTORS



Amit Tambe
Threat Researcher

**Attackers will continue to be crafty and innovative when devising tactics to trick users into infecting themselves. YouTube video descriptions could be the most lucrative, especially videos about gaming or pirating software. Both tend to attract unsuspecting victims, who—by the nature of what they are searching for—have questionable scruples, and who then become easy prey to attackers' tactics. In addition to YouTube, other crowd attracters such as Telegram, Discord, etc. will continue to be the first step for attackers wanting to spread their malware.**

# About F-Secure

F-Secure makes every digital moment more secure, for everyone. We deliver brilliantly simple, frictionless security experiences that make life easier for the tens of millions of people we protect and our 170 partners.

For more than 30 years, we've led the cyber security industry, inspired by a pioneering spirit born out of a shared commitment to do better by working together.

For more information visit F-Secure today.

F-Secure®