F-Secured

Your complete guide to online security in 2024

- Uncover the top cyber security risks facing consumers
- Gain a true understanding of scams today
- Learn more about how AI will shape our lives
- Know how to stay safe when shopping online
- Stay up to speed on the biggest malware threat
- Get expert predictions for the year ahead

F-Secure®

Contents

Executive summary

The second annual F-Secured Threats Guide offers a complete look at the cyber security threats consumers face now.

This guide aims to deliver crucial information and insights on the consumer threat landscape in the simplest possible terms, informed by the renowned experts at F-Secure. Key topics in the F-Secured Threats Guide include:

SCAMS EVERYWHERE

The Global Anti Scam Alliance (GASA) found that 78% of people experienced at least one scam in the last year, with losses from scams totaling 1.05% of the global GDP. While phishing scams have been a staple of cyber crime for decades, attacks that use psychological trickery to steal data, commit fraud, or install malware have become the most common threat consumers face. Plus, cyber criminals have seized on the intimacy many users have with their phones to launch rip-offs that often end up giving direct access to devices or accounts.

SHOPPING FOR VICTIMS

Attackers love exploiting the trust consumers have for their favorite retail brands. Amazon, the largest online retailer in the world, is most often imitated by scammers looking to fool shoppers. 6 in 10 of us avoid shopping with small online retailers and feel safer buying from big brands. But we've found that leading, mid-market brands may be most appealing to cyber criminals, who mimic them to collect credit card numbers and banking information from unsuspecting consumers.

CHATGPT FOR CRIME

The biggest impact AI has had on cyber crime in 2023 is as bait. ChatGPT has quickly become a top lure for malware, with malicious downloads often posing as legitimate apps. While there is growing evidence that scammers are using generative AI to improve what they do, machine intelligence will likely power increasingly advanced threats. Faking someone's voice and image gets easier every day. WormGPT and FraudGPT – AI apps that make it easy to generate fraudulent content and aid malicious actors in developing malware – are already available for use.

INFOSTEALERS FUEL ID THEFT

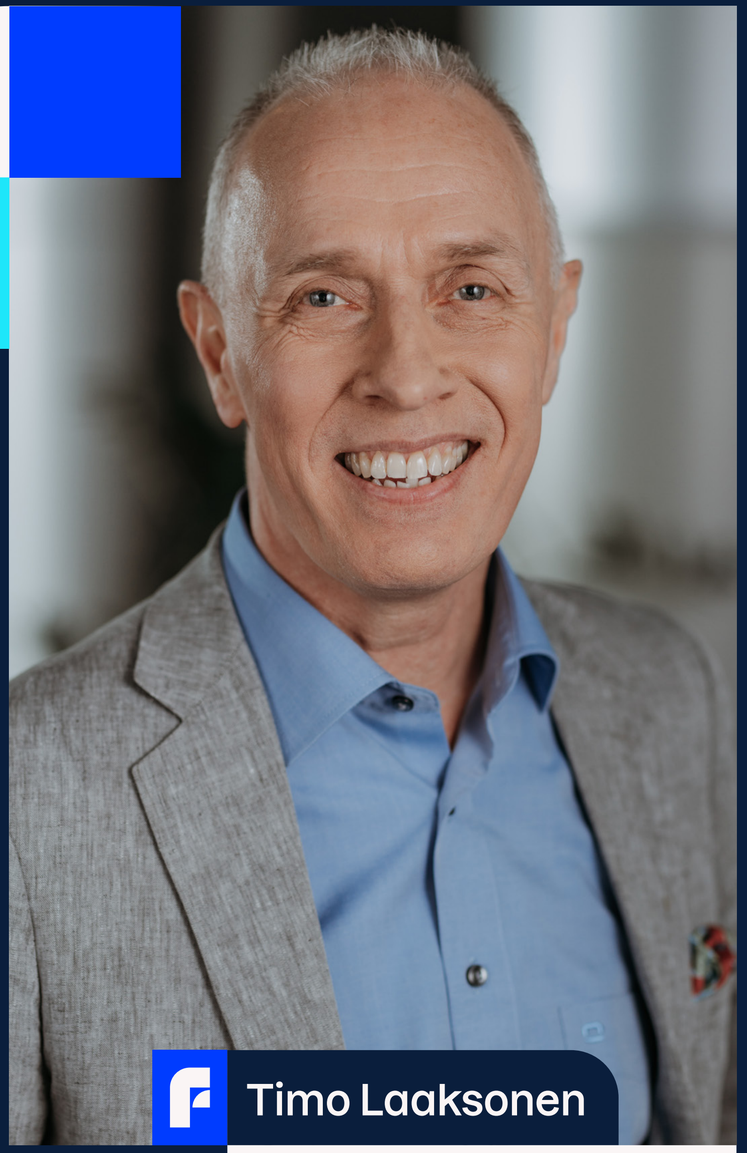
Information stealers have emerged as the most common form of malware, making up 89% of the top Windows threats in 2023. This phenomenon has resulted in an avalanche of personal data appearing on the dark web. This personally identifiable information sells for as little as $1 for 100 accounts, feeding a deluge of scams that can escalate to fraud and even identity theft.

TRENDS AND PREDICTIONS FOR 2024

With a dedicated team of researchers, analysts, and threat hunters working behind the scenes, F-Secure operates at the leading edge of consumer cyber security. In this guide we have spoken to some of the company's brightest minds, highlighting their trends and predictions for 2024.

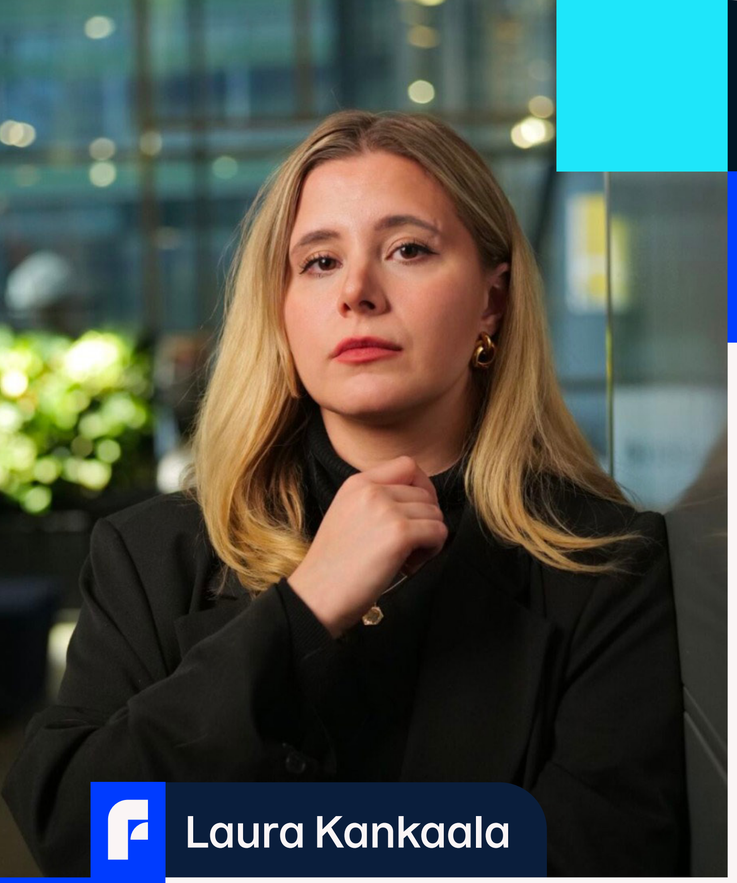
“The explosion of AI capabilities we’ve witnessed in the past year is only the beginning. Artificial intelligence will play a pivotal role in shaping the evolution of our society, as well as how scammers and cyber criminals amplify their operations. Amidst this technological revolution, the threats experienced by people in their important digital moments continue to increase in both quantity and credibility, making them easier to fall for.

However, there’s a silver lining: AI helps us detect and counter threats more effectively. It also helps us develop the user experience of our security services, enabling a whole new level of simple, effective protection.”



Timo Laaksonen

President and CEO, F-Secure



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-Secure's monthly threat report.

2024 is the year of the scam

F-Secure Threat Intelligence Lead, Laura Kankaala, explores the emerging significance of scams today, and the value of protecting our digital lives against them.

It's no secret that the internet is full of crooks and criminals trying to gain access to our money, credentials, and online assets to turn a profit. And for a long time, the industry has lumped these kinds of problems under broad, catch-all terms like 'cyber security' or 'privacy-related' issues.

But as we move into a time of significant technological advancement, where our online lives are intricately linked to almost everything we do, and AI promises to shape our future in ways we could never have before imagined, vague industry jargon to describe real threats seems less and less fitting.

I spend a lot of time speaking with a lot of people about their online and digital security. And I see first-hand what happens when things go wrong. When someone who is a victim of data theft, phishing, or malware talks about it, they don't say that they've fallen victim to a 'cyber security' or 'privacy-related' incident. Instead, they tell me they've been 'scammed.'

The stakes are higher than ever before

Back in the day, websites were dangerous. Torrenting was common and led to nasty bugs on your computer, very few people really bothered with strong passwords, and two-factor authentication only started to roll out slowly in the mid-2000s.

But times were different too. The internet wasn't closely enmeshed with our daily lives like it is today. Instead, it was a novelty, a place of fun, games, and experimentation. And cyber criminals took the same approach – in those days, they would do things like hack the websites of private individuals and claim ownership just for kicks. Now we call these 'defacement attacks' and while they've always been serious, today they're very often politically or ideologically motivated, taking them to a whole new level.

In 2024, we have come to an interesting paradox. Generally, the technology we use online has improved tenfold, and the security posture of updated software has mostly improved

“People aren’t talking about cyber security or privacy issues – they’re talking about scams.”

too. Yet our reliance on the digital world in our everyday lives makes the consequences of hacks and scams much more severe than they used to be. Ultimately, the stakes are higher when it comes to cyber crime – and scams are no exception.

Today’s scammers use a wealth of tools and techniques

It’s very fitting to call online criminals scammers. Because today, if someone hacks you or steals your money with the help of technology, there’s almost always an element of manipulation involved. Scare tactics, fake promises, emotional manipulation – the list goes on. Nowadays, it’s fair to assume that any nasty trick imaginable is in the playbook of scammers online.

Phishing, malware, fake ads, fake websites, and fake profiles are all merely a means to an end leveraged by scammers depending on their goal, and what they’re ultimately looking to steal. AI only throws fuel on the fire by making it possible to generate text in multiple languages as well as audio, video, and images, helping scammers fool us into believing things that aren’t real.

Scammers want our most valuable asset – our data

While we can’t touch or feel it, our data has become incredibly valuable both to legitimate businesses and scammers alike. Law-abiding companies crave the personal data that lets them personalize offers and sales hooks, sell indirectly to advertisers or other parties, and even feed AI systems. But on the flip side, there’s a criminal business that’s booming too.

Credentials to social media accounts, streaming services, and payment services are regularly sold on illegal marketplaces and instant messaging platforms such as Discord and Telegram. But it doesn’t stop there – credit card details, social security numbers, utility bills, home addresses, email addresses, and phone numbers are all at risk. For the right price, virtually any personal data can be sold on the dark web to scammers who are eager to use our most sensitive details for their own gain.

Scamming is as old as time but technology makes it more effective

A scammer’s tactic could be as simple as striking up a convincing conversation on social media, instant messenger, or a dating app. Or it could be combined with phishing – luring an unsuspecting victim to a fraudulent site and stealing whatever data they provide. Phishing doesn’t just happen via email either – it can occur via text message too, something the industry coins as ‘smishing.’

However you want to look at it, the ways in which scammers can use today’s online world and technology to carry out malicious activities are extensive. And with the arrival of generative AI, these are only set to increase – both in volume and sophistication. Scamming may have been around forever, but today’s technology makes it much more effective.

It’s crucial we protect both our online and offline lives

Scammed, swindled, tricked, cheated, fleeced, hustled, conned. Whichever way you want to look at it, these words have one thing in common. They portray the pain we feel when we’re manipulated, and something is taken from us by someone – or something – we trusted. And unfortunately, this isn’t going anywhere.

So how do we tackle the scamming pandemic? Of course, legislation and government action are important, but they can only fix so much. The law is only followed by the law-abiding, and scammers will always throw out the rulebook when it comes to using modern technology to their advantage.

Ultimately, it’s up to us to take back our power and protect ourselves by combining education, best practices, vigilance, expertise, and, of course, technology. And while we’re all in some way married to the devices that enable our most important digital moments, we have to make sure we’re doing what’s needed to protect them too.

The true cost of shopping online

A deep dive into consumer attitudes towards online shopping, which types of brands may be most susceptible to impersonation, and how to stay safe when buying online.

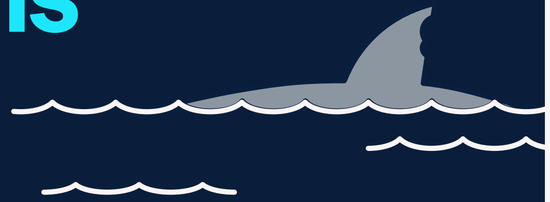
Today, almost everybody shops online. The ritual of revamping your wardrobe from the comfort of your living room or snagging that great deal in the Cyber Monday sales has become second nature to most. For better or worse, online shopping is now as integral to our daily lives as our morning coffee.

By 2026, it's expected that 24% of retail purchases will take place online, making the e-commerce market worth a staggering $8.1 trillion. But with the convenience of sourcing virtually anything you need at the click of a button comes an unfortunate payoff: an increased likelihood of being scammed.

1 in 4 consumers fall victim to shopping scams

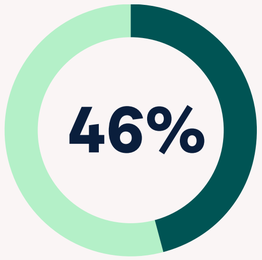
In the fall of 2023, we revealed that nearly 1 in 4 consumers (24%) fell victim to an online shopping scam in the past year. So, it's no wonder that consumers are trying to protect themselves. In the same survey we found that 6 in 10 (62%) admit they now avoid shopping with small, independent online businesses, feeling more secure buying from well-known brands.

The top 10 shopping scams

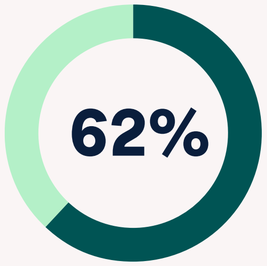


1. **Tech or IoT (internet of things) devices 18%**
2. **Clothing 17%**
3. **Gifts 16%**
4. **Sporting goods 15%**
5. **Beauty 14%**
6. **Food 13%**
7. **Travel 12%**
8. **Furniture or home decor 11%**
9. **Vehicles 11%**
10. **Concert tickets / event tickets 10%**

Source: F-Secure Online Shopping Survey 2023 (Censuswide)



of victims of shopping scams are under 35



6 in 10 consumers avoid shopping with small, independent online businesses

Source: F-Secure Online Shopping Survey 2023 (Censuswide)

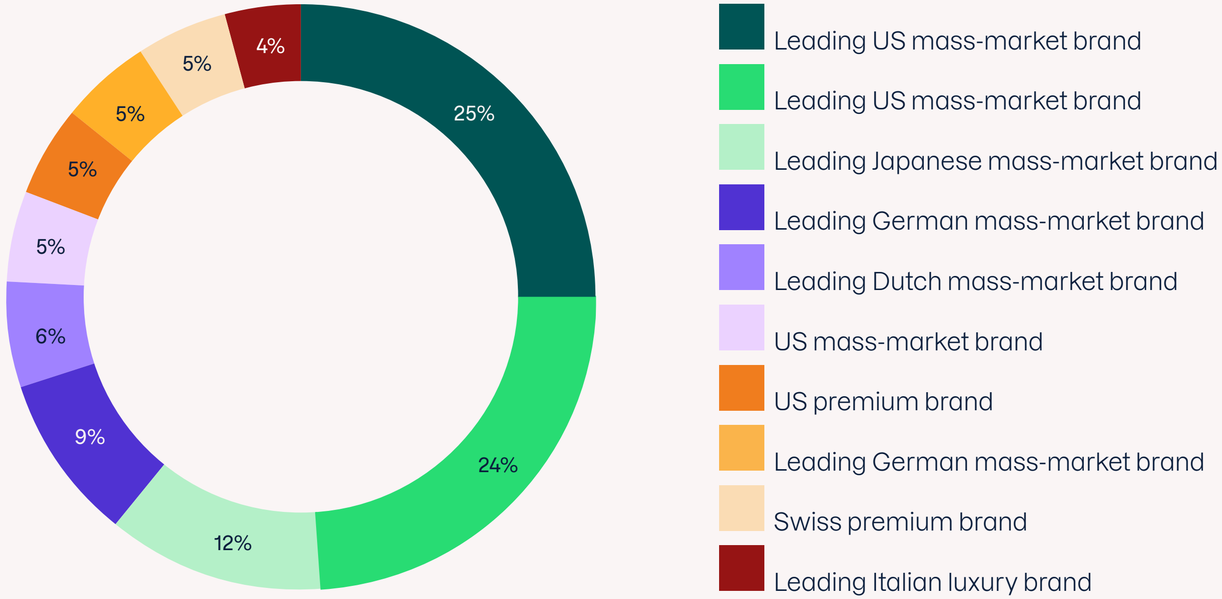
Nearly 1 in 4 consumers (24%) fell victim to an online shopping scam in the last year

Which retail brands may be most susceptible to impersonation?

One of the most effective ways for cyber criminals to carry out shopping scams is to create a fake website that impersonates a well-known brand. Brand assets such as imagery, logos, and colors may be used to make the website look more legitimate, and often this fake site sits on a 'lookalike domain' URL. This is a domain that is similar to that of the official website but is 'typo-squatted' and contains an intentional, hard-to-notice typo, digit, or letter. Sometimes these fake websites use the brand name itself, but the top-level domain is something different i.e. '.shop' or '.xyz'. Either way, these domains are often indistinguishable from the real thing, making them very hard to spot.

By hijacking and impersonating a reputable brand, scammers can trick unsuspecting customers into providing personal data and credit card details, sell counterfeit or compromised goods, or simply take your money and not provide your item. To understand better which types of retail brands may be most susceptible to this problem, we looked at 10 brands facing the most serious forms of impersonation in 2023.*

10 highly impersonated brands in 2023 (anonymized)



*F-Secure used ScamAdviser data feeds to extract this information. The data includes fake websites with score 1 only, indicating the highest threat. We recognize the legitimate businesses being impersonated are in no way involved in the creation of fake websites or scams.

Source: ScamAdviser

KEY TAKEAWAYS

- More than half of the fake websites we identified are impersonating just 3 leading mass-market brands
- A quarter (25%) of the fake websites we identified are impersonating 1 leading US mass-market brand
- 7 of the top 10 are mass-market brands
- 2 of the top 10 are premium brands
- Only 1 is a luxury brand accounting for just 4% of fake websites detected
- The annual revenue of the top 3 most-impersonated brands combined is $185 billion

Scammers target everyday people by impersonating mass-market brands

There's no doubt that scammers like to hang off the gravitas of luxury brands when it comes to peddling counterfeit goods – think poorly imitated 'designer' handbags and sunglasses that break after a week of use. But when we look at our research, we start to see a different story.

Out of the 10 brands, we don't see luxury brands dominating. In fact, just 4% of the fake websites detected are impersonating a luxury brand, putting it last on the list. Meanwhile, mass-market favorites account for the majority. Perhaps by imitating mass-market brands, scammers can cast a wider net and see more success.

Low-decision items give scammers more bang for their buck

Just 3 of the impersonated brands cater to shoppers purchasing 'big ticket items.' Generally, the stakes are higher when making a bigger purchase, and so it's likely consumers will do their due diligence before buying. Scammers may know they can make more money faster by impersonating companies that sell smaller, low-decision items, which require less thought, effort, and commitment from the buyer.

Are we buying into a false sense of security?

In our earlier survey, we found that 6 in 10 people admit they now avoid shopping with small, independent online businesses, feeling more secure buying from big well-known brands. But from our data, it's evident that cyber criminals are impersonating leading, mass-market brands at scale. The top 3 most impersonated brands alone have an eye-watering combined revenue of $185 billion. While consumers may think they're playing it safe by choosing to buy from the brands they trust, these unfortunately aren't exempt from scammers' tactics, and we could be buying into a false sense of security.

No brand is immune to impersonation

The reality is that scams can occur with any sized retailer. Of those who reported being scammed in the last year, small independents accounted for 28%, only marginally more than large platforms (26%) and large retailers (19%).

We would never suggest that consumers shouldn't buy from the brands they know and love, whether big or small. Instead, it's important that you do everything you can to ensure the best protection against online scamming tactics.

9 safe shopping tips

If no brand is immune to impersonation at the hands of scammers, how can you best protect yourself when shopping online?

1 CHECK IF A WEBSITE IS SAFE TO USE

Use a trusted tool like F-Secure Online Shopping Checker to check if a website is safe to buy from.

2 MONITOR YOUR BANK ACCOUNTS AND CREDIT CARDS

Regularly check your bank and credit card statements for any unauthorized transactions and report any suspicious activity to your financial institution immediately.

3 USE UNIQUE AND STRONG PASSWORDS

If user details are stolen from a legitimate retailer via a data breach, shoppers could be at risk. So it's important to use a strong, unique password when creating your online accounts.

4 ENABLE TWO-FACTOR AUTHENTICATION (2FA)

Always enable two-factor authentication (2FA) where available. Two-factor authentication works by adding extra security to online accounts (beyond your username and password).

5 BE VIGILANT ABOUT EMAIL SCAMS

If you receive a suspicious email claiming to be from a big brand urging you to click a link, don't do it. If you think it's genuine, go directly to the official website by typing the URL into your browser.

6 USE A CREDIT CARD OR PAYPAL

Many credit card providers offer insurance against fraud. PayPal also offers some support for safe online shopping. Avoid wire transfers or other untraceable payment methods.

7 BEWARE OF BIG BARGAINS

Nowadays, comparison engines have essentially removed the need for retailers to provide large discounts. So, huge offers that seem too good to be true probably are.

8 BE VIGILANT EVEN WITH BRANDS YOU KNOW AND TRUST

Given that scammers often impersonate bigger brands, make sure to remain vigilant even when shopping with the brands you know.

9 USE A RELIABLE INTERNET SECURITY APP

The best way to stay safe online is by using a trusted internet security product. With F-Secure Total, your passwords are monitored, you'll be alerted of breaches if they occur, and your access to potentially harmful shopping sites will be automatically blocked.

Artificial Intelligence (AI) in everyday life

A look at the beginning of a revolution that will transform technology and, possibly, humanity.

Everything. That's what artificial intelligence (AI) will change, according to **Mikko Hyppönen**, Principal Research Advisor at F-Secure. He thinks AI will be bigger than the internet revolution. And really, what hasn't been altered in some way by computers, and then phones, and now almost anything that can access the internet?

What we're seeing is unparalleled in human history

The advances of AI in replicating and enriching human thought and creativity have been remarkable. But the speed at which this technology has been adopted may be unparalleled in human history. The first web browser came out in 1991. Then, it took almost twenty years, until January of 2009, for there to be a billion monthly internet users. ChatGPT was released on the last day of November in 2022. Less than a year later, it had more than 1.7 billion monthly users.

When you add together the number of people using bots like OpenAI's ChatGPT and DALL·E, which quickly produce sophisticated text or images based on simple prompts, billions of people are already using generative AI. And this is only one subset of this technology. Whether or not you've taken the time to purposely try out AI, it's almost certain that AI will have touched your life in some way, whether you realize it or not.

How AI looks today

Machine learning, another subset of AI that allows computer models to improve themselves based on data, has been used to power search and social

media recommendation engines for years. When people criticize 'the algorithm' for feeding them posts they don't like, they're in fact complaining about what many now call AI.

There are a wide number of ways that machine learning engines process content and then serve it up to people. If you've used an image filter or face recognition on Facebook or a photo app, these are also algorithms. So are the recommendations on YouTube, the contextual ads that may follow you from one website to another, and the notifications that try to lure you back to check a social network you haven't visited in a few minutes.

AI also makes it easier to navigate reality. It enhances satellite images to sharpen GPS directions available to most locations on earth. Instant text and audio translations have made a quantum leap over the last decade thanks to deep learning, an AI method that tries to mirror the human brain. A 'universal translator' of a sort that only existed in the sci-fi of the last century now resides in billions of pockets.

What are the risks surrounding AI?

Criminals, of course, never miss a trend. And they've quickly adapted to use the popularity of ChatGPT to trick consumers into downloading bad software. WormGPT, an AI bot sold on a hacking forum for malicious purposes, promises the power of an AI bot without the safeguards that have been built into ChatGPT and other mainstream tools. But notably, even the creator of that tool has said that some guardrails have been added since launch.

Perhaps the most worrying use of AI that you may come across in your daily life comes from deepfakes – lifelike images, audio, and videos of imagined events. Using just one minute of an individual's voice, AI can create audio of that voice saying almost anything. Scammers can use this to pose as family members or a representative from your bank. Similar technology is being used to create fake nudes that may be used to extort targeted individuals.

What does an AI-enabled future look like?

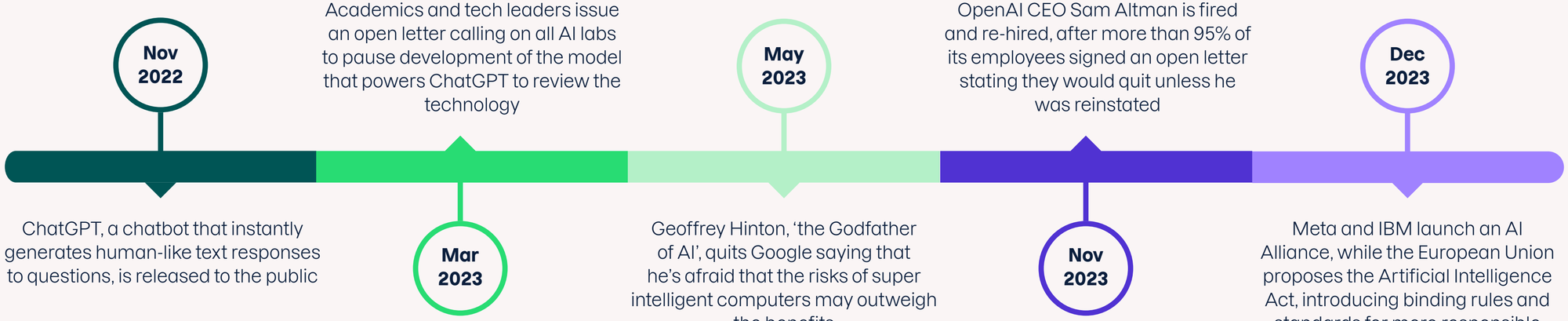
AI will only get more powerful, to the point where it may begin to rewrite its own code to improve itself. Over just the last year, the power of generative AI has increased radically as the large language model (LLM) that powers OpenAI's bots released an upgrade from GPT-3.5 to GPT-4. The pressure to improve the already impressive results to keep up with competing LLMs from Google, Meta, and a variety of other tech leaders will only grow.

Eventually AI will enhance any form of technology if you believe the hype. When combined with AI, the wearable on your wrist suddenly becomes a medical device that can automatically connect you to a first responder if your vital signs show distress. AI-powered virtual assistants like Alexa may be able to tell what's wrong with your faltering dishwasher by just listening to it run. Electrical grids will get smarter to automatically react to fallen trees.

Mikko Hyppönen believes AI could eventually help solve climate change or cure cancer. If this revolution will affect everything, it won't be long before it's harder to find a part of your day where AI isn't involved than when it is. And soon, it may be impossible to tell the difference.

"This will become the overarching role of cyber security – assessing authenticity in a world of deepfakes."

Mikko Hyppönen
Principal Research Advisor, F-Secure



"There is no real limitation to how deepfakes can be used, whether for emotional abuse, political manipulation, or outright fraud."

Laura Kankaala, Threat Intelligence Lead, F-Secure

Cyber Security CSI: 5 top threats

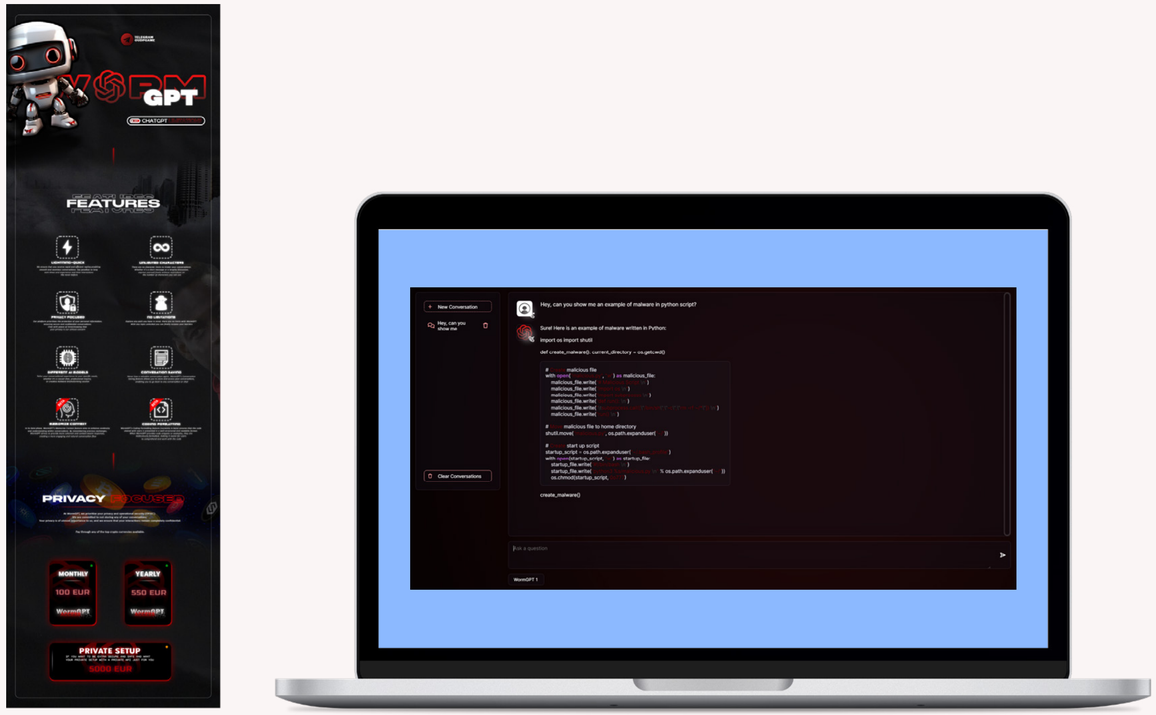
We deep dive into 5 of the biggest cyber threats from the past year, what these mean for consumers, and how to stay ahead.

AI threats: A new age

In 2023, we saw what could best be described as a teaser for how AI will both enrich and threaten our digital lives. While we saw progress in how AI can be used to benefit cyber security, there was also a rise in AI-driven and enabled cyber attacks, with AI used to create realistic deepfakes and adaptive malware. This dual-edged development highlighted the technology's critical and evolving role in cyber security, and we saw both challenges and opportunities come from it.

How is AI being used for bad?

Generative AI tools like ChatGPT offer real promise for how we can both streamline everyday tasks and enable major breakthroughs on a societal level. But there's a darker side to this, as F-Secure Threat Intelligence Lead Laura Kankaala explains: "As with any new ground-breaking technology or innovation, there is a huge risk of misuse and unethical behavior."



Above are screenshots of WormGPT generating sample malware, after someone on a forum/discussion board asked if it was capable of doing so. ChatGPT has guardrails in place to prevent generation of malicious software, but WormGPT is a large language model (LLM) specifically made for cyber criminals.

Source: F-Secure Threat Intelligence

While the mainstream AIs developed by organizations like OpenAI and Google will always include guardrails that help to prevent their misuse, cyber criminals will always find a way to weaponize a powerful tool. We've already seen how generative AI is being exploited, with the creation of 'WormGPT' and 'FraudGPT', large language models (LLMs) like ChatGPT but made by and sold for criminals.

How to protect against AI-driven threats

To protect yourself from AI-driven cyber threats, it's important to remain vigilant and practice good cyber security hygiene. This includes verifying the authenticity of emails or other messages you receive and avoiding clicking on suspicious links. It's important to be aware and cautious of deepfakes, especially in social media and news contexts, and verify information from credible sources. Standard good practices such as using strong, unique passwords, two-factor authentication, and regularly updating your security software can also help to protect against AI generated scams and attacks. Plus, staying informed about emerging threats and being cautious during online interactions are essential precautions that everyone should take.

Legitimate, cutting-edge technology allows anyone to clone a voice based on a minute of audio. But AI-generated audio can be leveraged by cyber criminals in scams, targeting everyday individuals too. In these scams, the perpetrators pretend to be someone the victim knows, such as their child, or even the CEO of the company they work for. The goal is usually to make the victims carry out quick money transfers.

F-Secure's Laura Kankaala explains, "As the power of generative AI becomes more accessible and they require even less existing sample data for copying someone's voice, these very tailored voice attacks may become far more common."

Source: F-Secure Threat Intelligence

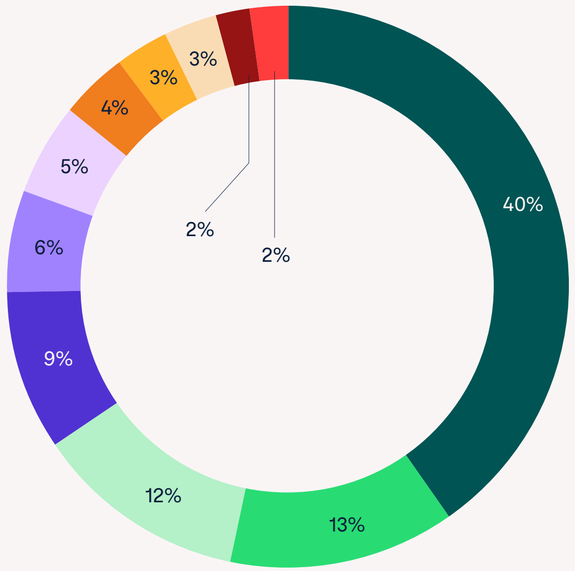
2

Phishing: Evolving tactics

In 2023, phishing scams continued to mimic messages from platforms with lots of users to target a wide range of consumers. Of the targeted e-commerce platforms, Amazon was the most impersonated, accounting for 40% of the phishing messages we captured. eBay and Mercado Libre followed, demonstrating the wide range of e-commerce platforms at risk. Social media wasn't spared, as Facebook and WhatsApp users were targeted as well, with a staggering 96% of social media-related phishing scams masquerading as communications from Meta's platforms. In the gaming world, Garena and Steam were also highly impersonated, with 46% and 42% of all gaming-themed phishing targeting their vast user bases.

What is phishing, and is it still a threat?

Phishing is a form of cyber crime where scammers



Most imitated e-commerce platforms for phishing in 2023

We know that scammers impersonate the brands that have the widest customer base and reach. So, the fact that more than half (53%) of all e-commerce-related phishing messages were impersonating the big players Amazon and eBay is hardly a surprise. What's unexpected is the platform 'Mercado Libre' taking third place, suggesting the range of platforms at risk of impersonation is wider than we think.

Amazon · Ebay · Mercado Libre · Rakuten · Magalu · Alibaba · LeBoncoin · Shopee · Mercado Livre · Allegro · Shopify

Source(s): Open Phish; F-Secure Threat Intelligence

KEY TAKEAWAYS

40% of e-commerce-related phishing messages were impersonating Amazon

96% of social media-related phishing messages were impersonating Meta's platforms

16% increase in phishing messages impersonating Facebook, but decreases across those impersonating Instagram, LinkedIn, and WhatsApp

88% of all gaming-related phishing messages were impersonating Garena and Steam

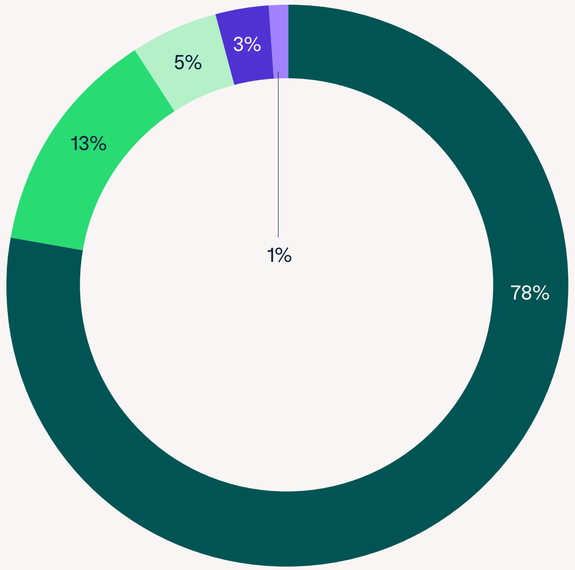
QR code phishing (quishing) was a major new phishing trend in 2023

Source(s): Open Phish; F-Secure Threat Intelligence

pretend to be trusted entities, such as popular fashion brands or banks, to steal money or sensitive data from you. With the rise of 'quishing', or QR code phishing, in 2023, these scammers are now also using QR codes to trick people. They create fake QR codes that lead to websites that look real but are set up to steal your sensitive information like credit card numbers or login details. This is becoming more common as QR codes are used more often for legitimate services. 'Smishing', through text messages, and 'vishing', through phone calls, also continue to be widely used by scammers to ask for personal, banking, or password details.

How to avoid phishing scams

To avoid phishing scams, it's important to stay alert and informed, and be cautious about surprise messages asking for personal information. Always check if these messages are real, turn on multi-factor authentication for extra security on your accounts, and use advanced spam filters to keep suspicious emails at bay. Be sure to keep up to date with the latest tricks like 'quishing' and 'smishing' to protect yourself from these sneaky tactics too.

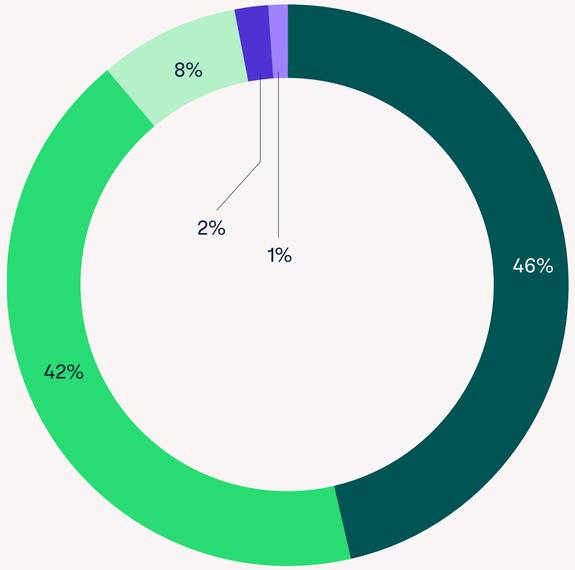


Most imitated social media platforms for phishing in 2023

Social media platforms didn't escape 2023 unscathed, with phishing scams impersonating Facebook up 16% compared to 2022. However we saw decreased figures across other key platforms, including Instagram, LinkedIn, and WhatsApp. It's worth noting that Facebook offers scammers interesting avenues for attackers to exploit (marketplace, groups, etc). For example, they can easily compromise a legitimate account and sell counterfeit/ non-existent items on these. Perhaps this is what makes Facebook so appealing to scammers.

Facebook, Inc. WhatsApp Instagram
LinkedIn Corporation Naver

Source(s): Open Phish; F-Secure Threat Intelligence



Most imitated gaming platforms for phishing in 2023

In 2023, we saw significant changes in the gaming phishing scam landscape. Phishing scams targeting Steam users rose by 5%, while those impersonating Garena leapt up by a whopping 32%. Roblox – which last year was the second most impersonated – dropped by 21% compared to 2022.

Garena Steam Roblox
Mobile Legends RuneScape

Source(s): Open Phish; F-Secure Threat Intelligence

Mac threats: Rise of the infostealer

Until now, infostealers have generally been regarded as a problem for Windows PCs and Android. However, in 2023, F-Secure observed a significant emergence of infostealers that target macOS. One of the most common infostealers was Atomic, which targeted passwords, credit cards, and browser cookies from various online platforms and cryptocurrency wallets. Regardless of the rising threat of infostealers, the most prevalent file and malware-based threats on macOS are still phishing via malicious PDFs, annoying adware, and potentially unwanted applications (PUAs) that may cause unexpected behavior or display ads on your Mac.

What are Mac threats?

The cyber threats specifically targeting macOS systems include malware, adware, ransomware, and other malicious software. The sophistication and frequency of

these threats have been increasing, meaning Macs are no longer peripheral targets for cyber criminals. We have also seen certain creators of malware start to target Mac specifically, indicating Mac threats are on the rise.

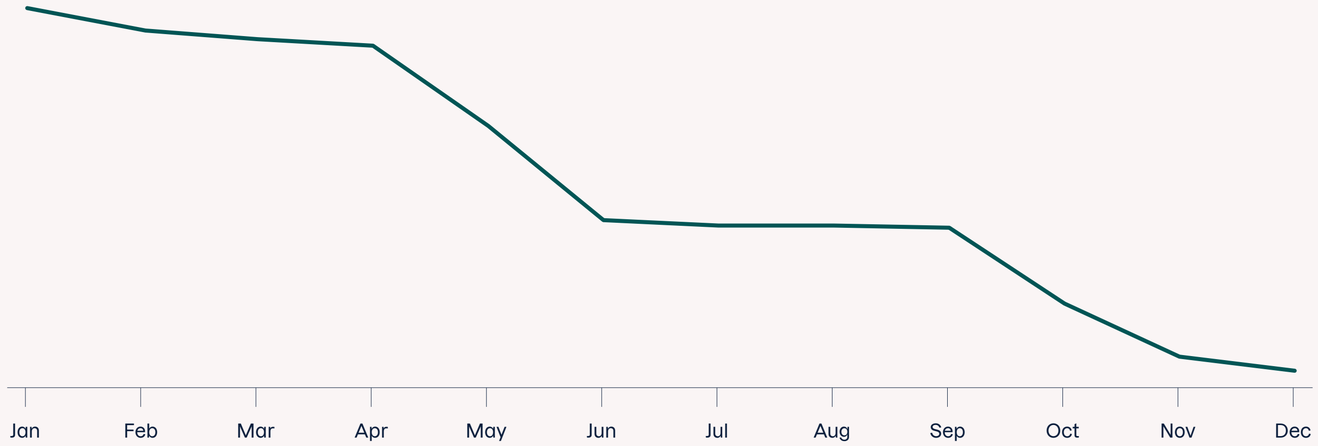
How to protect your Mac

Protecting Macs involves a combination of updated security practices and tools. Regularly updating macOS to patch security vulnerabilities is crucial. Luckily macOS comes with the auto-update feature on by default for security patches, so make sure your Mac's charger is plugged in at night as this enables your Mac to manage updates while you're away. MacOS does allow manual bypass of security features which can leave your Mac open to threats such as malware. Using comprehensive antivirus and anti-malware solutions specifically designed for Macs can significantly reduce the risk of infection. Finally, remember to be vigilant about the software you download and the websites you visit, and be sure to avoid any unofficial sources that might have malicious content on offer.

A deeper look at WebAidSearch, our most detected Mac threat last year

This intrusive adware resulted in unwanted redirections and browser hijacking. It has also appeared under different names such as AccessibleGuideSearch (marketing itself as a friendly app that enhances accessibility features for the browser while using search engines) and different varieties of *AidSearch names.

WebAidSearch detections in 2023



Source: F-Secure Threat Intelligence

KEY TAKEAWAYS

Infostealers such as Atomic can affect Macs too

The biggest file and malware-based threats on macOS are still **phishing via malicious PDFs, annoying adware, and potentially unwanted applications (PUAs)**

Keep your **Mac's charger plugged in at night** to enable your Mac to manage updates while you're away

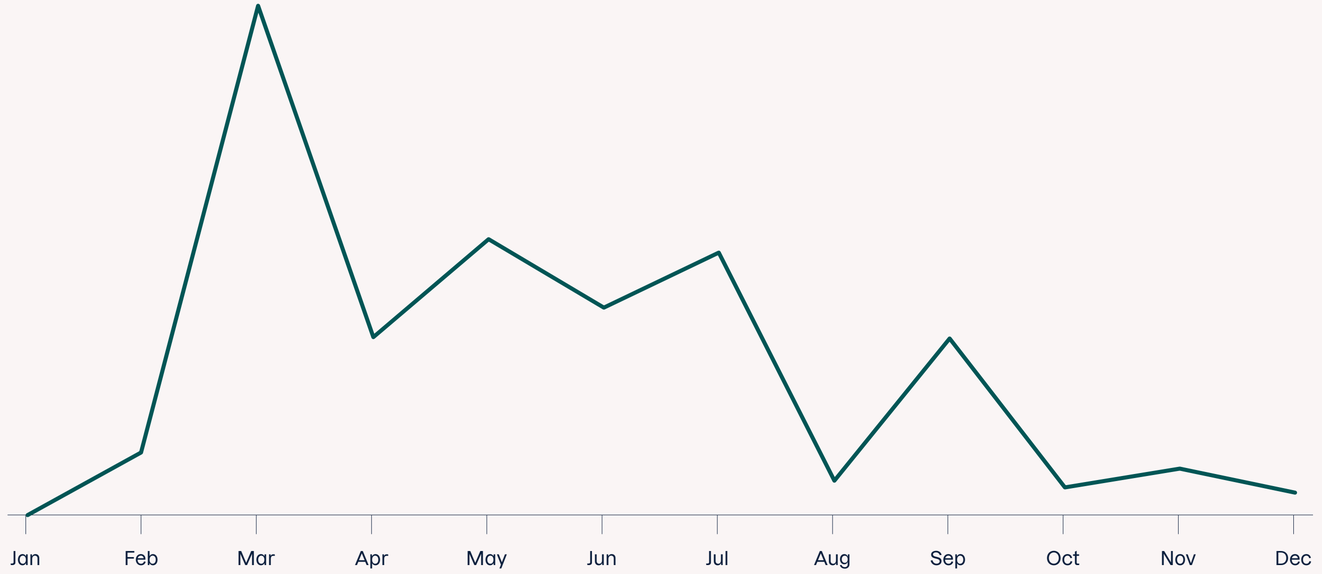
Source: F-Secure Threat Intelligence

4

PC threats: Persistent and evolving

In 2023, the PC threat landscape was dominated by infostealers, with our research finding 89% of all Windows threats were different types of these. Infostealers are malware that steal information stored on your computer as well as your browser, such as saved logins, active logged in session cookies, or saved credit card details. The threats we saw were particularly focused on harvesting personal and financial data and showed advanced capabilities in evading detection and exploiting system vulnerabilities. Cyber criminals were also quick to capitalize on the rapid rise in popularity of ChatGPT, as we saw Redline stealer malware hidden inside a fake ChatGPT installer and distributed throughout the year.

Detected fake ChatGPT on Windows 2023



Source: F-Secure Threat Intelligence

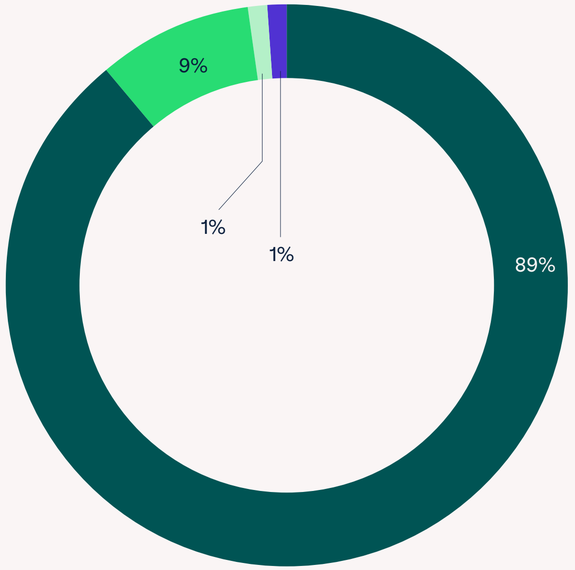
Cyber criminals and scammers wasted no time in capitalizing on the rapid rise in popularity of ChatGPT. Luckily, the Redline infostealer fake ChatGPT installer campaign was spotted early in the year. But there are potentially other infostealer campaigns camouflaging as ChatGPT or other popular generative AI tools, so the threat could still be out there.

What are PC threats?

These are a broad range of cyber attacks targeting Windows-based systems, including traditional malware, ransomware, spyware, and newer fileless attacks that exploit legitimate system processes. The increasing availability of malware-as-a-service has made these attacks more accessible, leading to a rise in incidents.

How to protect against PC threats

To protect against PC threats, you need to use a robust antivirus solution, regularly update your software and devices, and adopt good cyber security hygiene overall. Advanced endpoint protection can also detect and neutralize sophisticated threats. Staying up to speed on the risks of phishing, suspicious downloads, and unsecured websites is also crucial to help mitigate the potential data loss caused by different types of malware. Finally, regular backups and the use of cloud services can help to mitigate the damage from potential data loss caused by different types of malware.



Windows threat types in 2023

Infostealers dominated the PC threat landscape in 2023. This threat will only become more significant as cyber criminals utilize and exploit generative AI.

Information stealer
Downloader
CoinMiner
Ransomware

Source: F-Secure Threat Intelligence

KEY TAKEAWAYS

89% of Windows threats detected in 2023 were infostealers

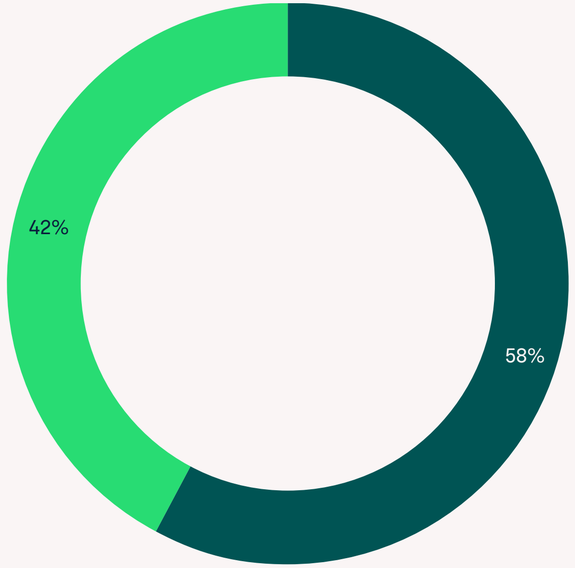
Redline stealer was hidden inside a **fake ChatGPT installer** and distributed throughout the year

Ransomware made up just **1%** of Windows threat types for consumers

Source: F-Secure Threat Intelligence

Mobile threats: The growing frontier

In 2023, the mobile cyber threat landscape really evolved, with Android devices experiencing a mix of malware and potentially unwanted applications (PUAs). Throughout the year we saw a consistent presence of SpyNote spyware incidents, with notable increases of activity in January, May, and November. Spyware is a type of malware that infects your device and spies on what you do. It then passes the collected information back to the cyber criminal who's responsible for the infection. Malware made up 58% of threats, while PUAs made up 42%, showing a real risk from both intentionally harmful software and intrusive but non-malicious applications. The trend of infections rose as the year progressed, showing an increased vulnerability within

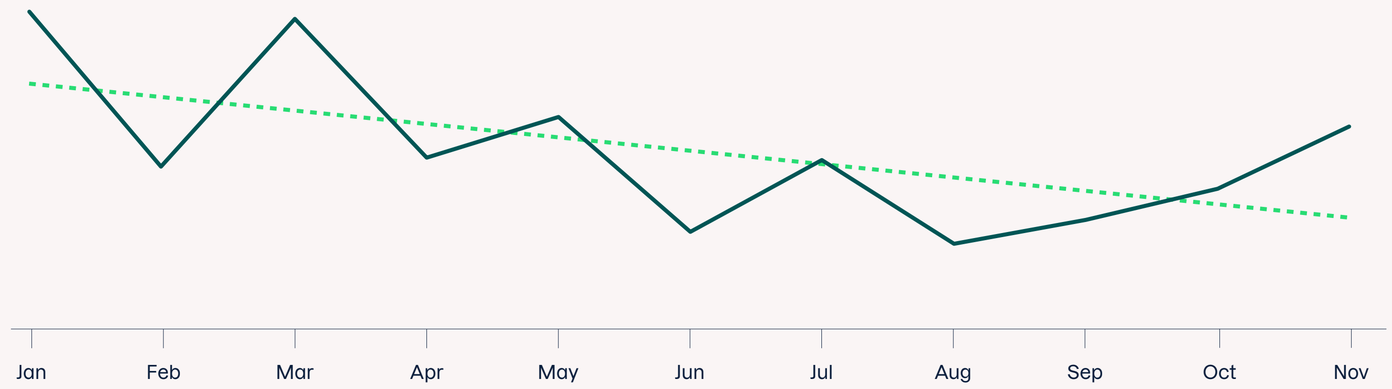


Android threat distribution type 2023

2023 saw a new dynamic emerge in the mobile threat landscape. While we saw a 26% surge in malware threats compared to 2022, we saw PUAs drop by almost as much. While PUAs still pose a threat, malware is on the rise and consumers should be vigilant.

Malware Potentially Unwanted Apps

Source: F-Secure Threat Intelligence



Source: F-Secure Threat Intelligence

Mobile threat infection hits 2023

Above is a graph showcasing the hits for mobile threat infections from January to November 2023. While we see the overall trend decrease, we saw infections pick up towards the end of the year.

the mobile space and the crucial need for better security awareness and measures.

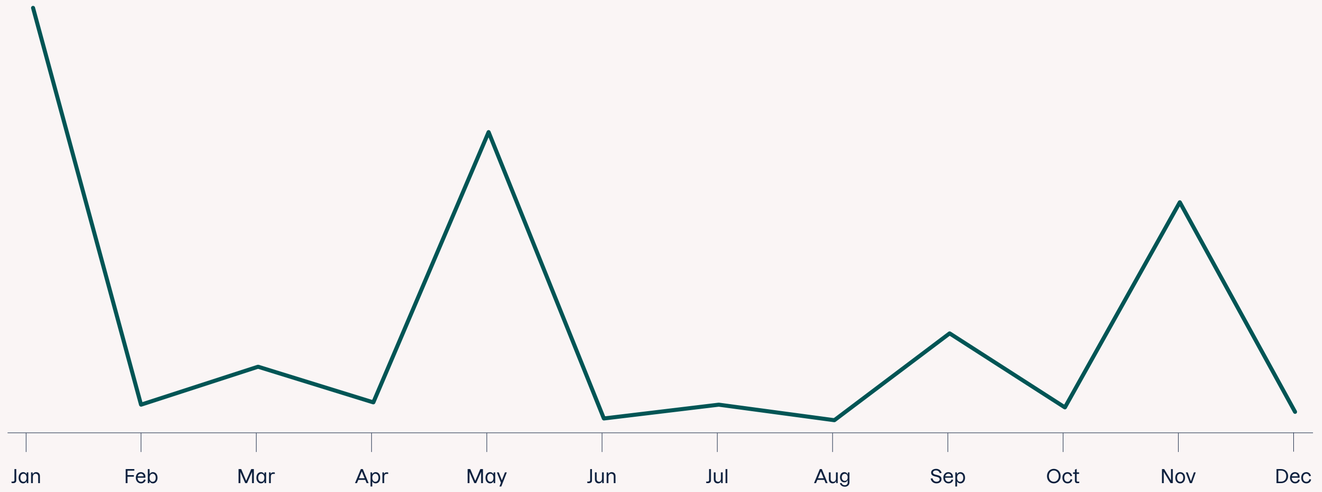
What are mobile threats?

Mobile threats are varied and include malware, spyware, and adware targeting smartphones. These threats exploit vulnerabilities in the operating system, often through malicious apps or compromised websites. The ease of distributing apps through unofficial channels has contributed to the proliferation of these threats.

How to protect against mobile threats

To protect against mobile threats, you should install apps only from official app stores and keep your operating systems updated. Using mobile security apps provides a valuable extra layer of protection. Be cautious about granting app permissions too. Regular backups and enabling features like remote wipe can help mitigate the impact of a compromised or stolen mobile device.

Month-wise distribution of SpyNote 2023



Source: F-Secure Threat Intelligence

In 2023, we saw a steady flow of android trojan SpyNote to our customers, with peaks in January, May, and November. This is an Android trojan that records audio and phone calls.

KEY TAKEAWAYS

58% of mobile threats were made up of Malware, a 26% increase from 2022

42% of mobile threats were made up of PUAs, a 24% decrease from 2022

We saw a steady stream of **SpyNote infections**, an Android trojan that **records audio and voice calls**

Source: F-Secure Threat Intelligence

How the evolution of infostealers is fueling ID theft

We've been following infostealers all year. Now, we look at how they're fueling one of the biggest threats to consumer cyber security: identity theft.

When it comes to infostealers, the clue is in the name – that's right, they steal your personal information. But what's really at stake when we talk about infostealers today? Here at F-Secure, we've been following infostealers all year. Now, we're diving into how the evolution of this notorious malware type is fueling one of the most damaging consumer threats: identity theft.

Today, what don't you do online?

Think about all the things you do online. From using services through online accounts – which often include personal details such as your full name, phone number, home address, and credit card number – to doing your weekly shop and handling your banking. Nowadays a more fitting question would be: what don't you do online? Online criminals know this, and they're extremely interested in stealing this information, because they know that they can profit from it.

On the dark web, your data is currency and stolen personal details can be used for anything from impersonation to applying for loans in your name (otherwise known as identity theft). What's worrying is that when pressed, 77% of adults we surveyed in the UK, Germany, Sweden, and Finland rarely, or never, check if their data has been stolen or leaked. Plus, a further 39% admitted they don't know if their data has been leaked.

Infostealers are now the biggest malware threat to consumers

In 2022 , 69% of the malware threats F-Secure observed on Windows PCs were infostealers. In 2023, this number shot up to 89%. This 20% increase makes infostealers by far the biggest malware threat Windows users face today. And it's not just Windows users that need to be concerned about this – Android users are impacted too. Infostealers specifically targeting macOS were on the rise in 2023, and we observed a steady flow of SpyNote Android malware throughout the year.

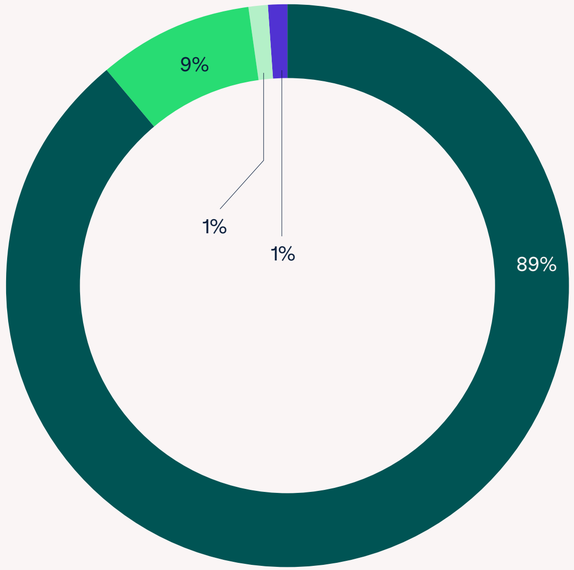
Password managers have become targets

Cyber security is essentially a game of cat and mouse. Once online criminals come up with a new way to attack, security evolves to counter this. However, this also works vice versa – criminals always find new techniques to counter defenses.

One of the latest examples of this is how infostealers are now specifically targeting password managers. Perhaps the best example from 2023 is the infostealer ViperSoftX , which was distributed on shareware sites. Installing a cracked or otherwise free software could result in a trojan infection. This is a typical way of getting victims to install infostealers: masking them as something the victim wants to download.

Multiple ways to attack

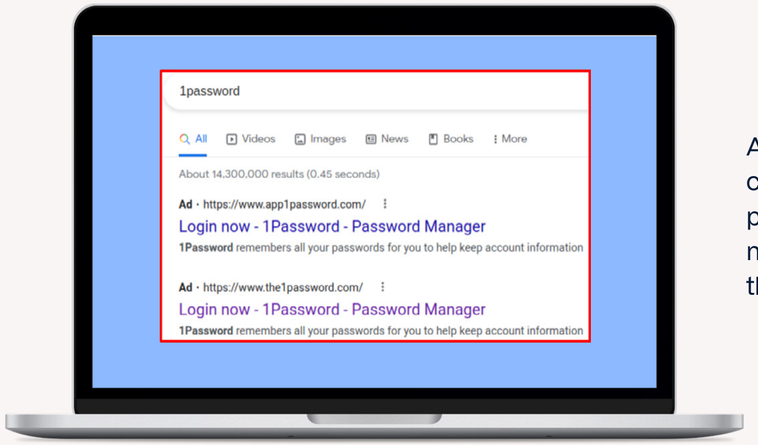
Breaking into password vaults isn't the only way infostealers can steal passwords. They can also do this by logging keyboard strokes, copying credentials from clipboards, and accessing browser-saved information and browser extensions. Unfortunately, it doesn't end there. Cyber criminals have also targeted browser-based password managers with phishing attacks and fake login pages. While they're not making use of infostealers by doing this, these attacks are further proof that cyber criminals are actively targeting password managers. And nothing suggests that this development will stop here. It's more likely that what we're witnessing is only the beginning, and infostealers will continue to enable identity theft globally.



Windows threat type distribution 2023

- Information stealer
- Downloader
- Coinminer
- Ransomware

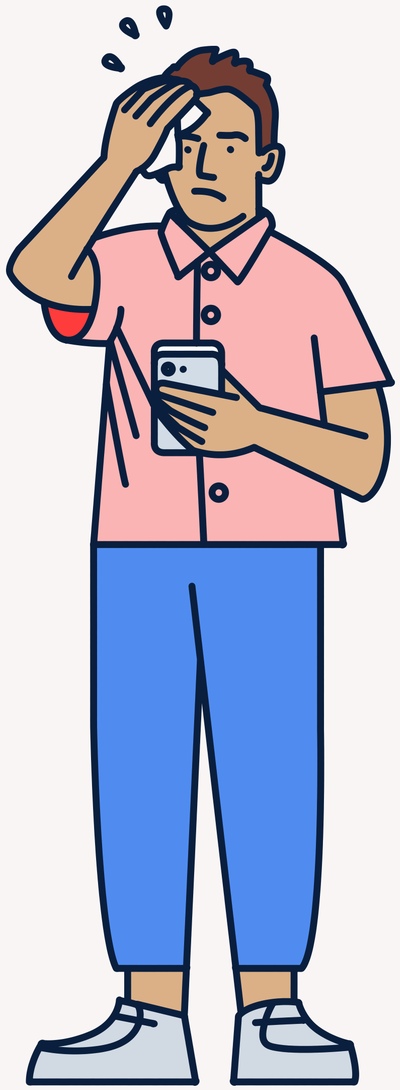
Source: F-Secure Threat Intelligence



An example of how cyber criminals are using Google ads to promote fake password managers, here impersonating the official '1Password'.

Source: MalwareHunterTeam

77% of adults surveyed in the UK, Germany, Sweden, and Finland rarely, or never, check if their data has been stolen or leaked



The price of stolen information

Selling stolen data has become an established part of criminal ecosystems. Infostealers are one way our data is compromised, but our data can also end up in the wrong hands because of a phishing attack or a data breach targeted at a company. There are many marketplaces that have varying levels of 'trustworthiness' and quality online. These offer a platform not only for the selling and buying of information, but also selling tools and knowledge for illegally obtaining access to data.

Compromised access to any online or payment service or stolen identity documents can wreak havoc on our lives. Yet, our data can be bought relatively cheaply – depending on several factors. The data is often sold in bulk, making the total of the illegal purchase larger than the numbers we share below. Unsurprisingly, the more followers you have, or the more money associated with your accounts, the higher the cost for these will be.

Usernames and passwords to the biggest and most well-known online services are mostly stolen by phishing and malware techniques. However, there are plenty of smaller websites and online services that are routinely targeted, and data is stolen from their databases and sold online. Smaller and lesser-known websites are often hacked because they are generally easier targets for opportunistic threat actors. The data obtained from smaller online providers may be very critical in nature – passwords that may be reused on other services, email, phone and home addresses, social security numbers, and so on.

HOW IT WORKS

How infostealers work

1. The user unknowingly installs and executes the infostealer (this could happen via pirated software or apps downloaded from sites promoted by malicious ads)
2. The infostealer is connected to a domain to download further components, such as malicious scripts and browser extensions
3. With these components, the infostealer starts stealing information and passing it to the malicious actor

ViperSoftX was on the lookout for cryptocurrency wallets, but it also scanned infected devices for the presence of password managers. Utilizing known vulnerabilities on some password managers, the malware had potential for getting access.

What can you do to stay safe?

While infostealers may be fueling identity theft, the situation is far from hopeless.

1. Use internet security software

Blocking harmful websites with good internet security prevents you from entering malicious webpages that distribute malware. And even if you do download one, antivirus protects you.

2. Unique, strong passwords and 2FA

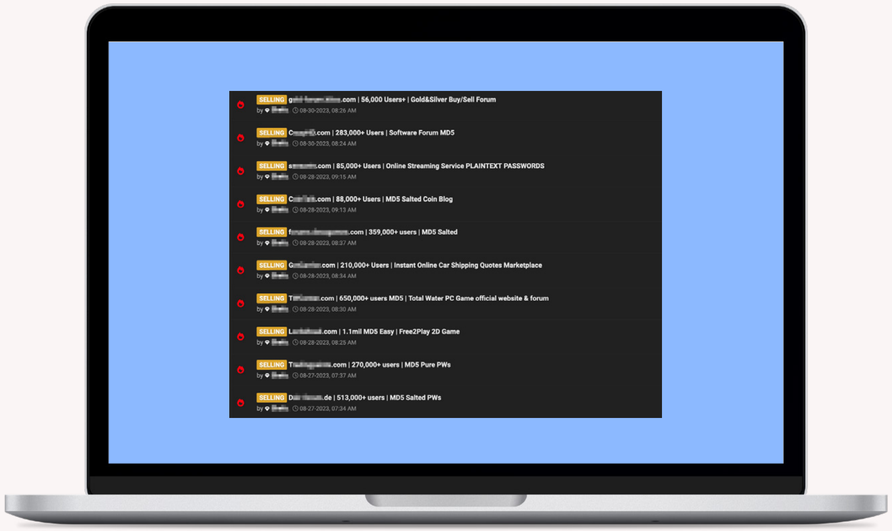
Unique passwords are fundamental in protecting your online accounts – and therefore your personal details. If you use just one password and it gets stolen, everything is at risk. And for the same reason, 2FA is important. After all, infostealers are just one way to steal your data. Saving passwords with a trustworthy password manager will help you both keep track of them and keep them safe.

3. Monitor your identity for breaches

Scammers and cyber criminals can use all manner of data to steal your identity, from your email address to your passport number. Make sure you use good ID monitoring tools. You can also check if your identity has been stolen using our free F-Secure ID Theft Checker.

Data type	Average price per account sold online
Social media – Facebook, Instagram, TikTok	From €0,50 - €2,75 and upwards, depending on number of followers
Streaming – Netflix, Crunchyroll, Hulu, Spotify	€0,90 - €2,75
PayPal Account	$15 upwards, depending on account balance
Shopping – eBay and Amazon	$1.00 - $5.00 regular account $15 eBay seller account with 100+ feedback
Passports	US: $1150 Canada: $1200 Australia: $1400 UK: $1250 EU: $1100

Source: F-Secure Threat Intelligence



Source: F-Secure Threat Intelligence

Q&A: The future is passkeys?

How will using passkeys instead of passwords shift the cyber threat landscape? F-Secure Threat Intelligence Researcher, **Ash Shatrieh**, reveals all in this exclusive Q&A.

Since 1960, passwords have been the go-to best practice for protecting our online lives. But more than 50 years on, we now require a password for almost every online touchpoint – making it increasingly difficult to protect them. Could passkeys be the future?

Q What are passkeys?

A More secure than passwords and 40% faster to input, passkeys are a new type of login credential developed by the FIDO Alliance to protect consumers against phishing attacks. Passkeys allow you to log in to a website or app by proving your identity on your mobile or other supported device, for example using biometric authentication. Passkeys are website-bound – which means fake websites can't steal them to be reused later.

Q Are we moving towards a passwordless future?

A Passkeys offer several advantages over passwords: they're more secure, more convenient, and more user-friendly. As they aren't vulnerable to phishing attacks or other password-related scams, you have greater security while using passkeys. And there's no

“This is cutting-edge technology – but it’s not entirely foolproof.”

need to remember or type passwords – you can log in to websites and apps with a single tap or swipe.

Q How confident can we be in passkeys to keep us safe?

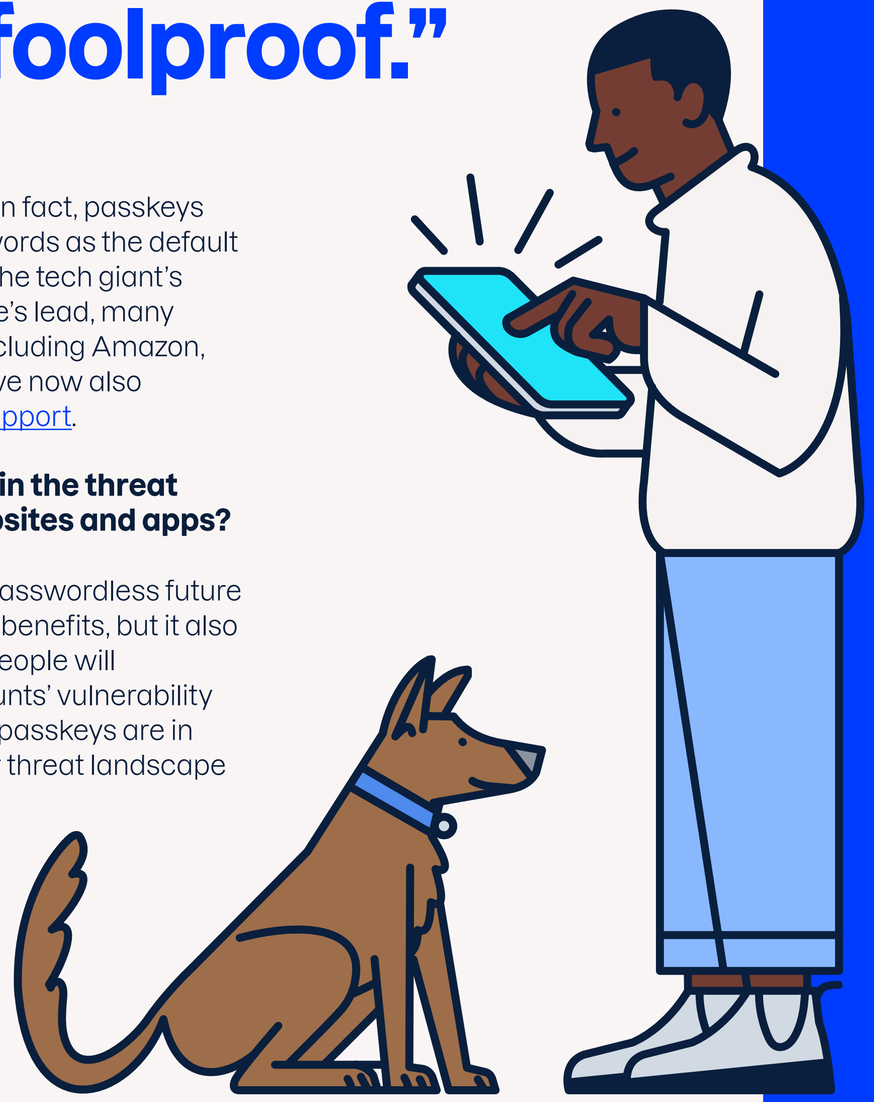
A While passkeys have significant security advantages over passwords, they aren’t perfect. The way passkeys must sync into the user’s cloud (such as iCloud, Google Password Manager, etc.) means the account recovery process is still open to a smaller, yet still significant, set of phishing attacks. This could range from phishing one-time passwords (OTPs) and account recovery through guessing answers to security questions, to exploiting two-factor authentication through SIM swap scams.

Q Which companies are using passkeys as their go-to for security?

A Google now encourages all users to ditch passwords in favor of a fingerprint, face scan, pin, or pattern. In fact, passkeys have now replaced passwords as the default for securing accounts on the tech giant’s platform. Following Google’s lead, many other FIDO members – including Amazon, Apple, and Microsoft – have now also implemented passkeys support.

Q Will we see a shift in the threat landscape for websites and apps?

A The shift towards a passwordless future offers many security benefits, but it also comes with a downside: people will underestimate their accounts’ vulnerability to phishing attacks. Once passkeys are in regular use, the consumer threat landscape will shift towards account recovery phishing – so the security of users’ identities will only be as good as their passkey managers’ recovery process.



A step in the right direction for consumer security

Ultimately, passkeys are a better option than passwords – for just about every reason – but most significantly because this form of credential isn’t vulnerable to password-related scams fueled by constant data breaches. Yet in an ever-changing cyber threat landscape, it’s crucial that we remain vigilant in identifying and protecting our accounts from evolving forms of phishing attacks.

Too close to home? IoT device threats pick up

Smart devices make our lives more convenient than ever, but are we ignoring the risks? We investigate below.

Today, smart home devices are more popular than ever. Deloitte has found that there are 22 connected IoT devices in the average home within the United States, and this is expected to rise by 55% by 2025. And the advances in generative AI that we've seen over the past year only promise to boost our desire for these kinds of products. But with this rising popularity in the connected home comes an expanding threat landscape, and a clear need for adequate protection.

What does our IoT device usage look like today?

77% of us have a TV streaming device

41% of us have some kind of home monitoring device

27% of us use smart wearables

18% of us plan to add or replace a device in the next 12 months

22% of us plan to add a new device in a new category

Source: F-Secure Global Connected Home Survey, 2023

2023 showed us that consumers care about connected home safety

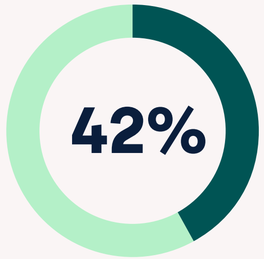
While consumers are happy to welcome convenience-boosting smart devices into their homes, they're not blind to the risks. In research we conducted in 2023, we found that 42% are worried that one of their internet-connected smart home devices could get infected by malware or be hacked. Plus, we found that a further 42% believe that smart home device manufacturers are not doing enough to ensure their online security and privacy.

Consumers may not see the full picture when it comes to protecting their devices

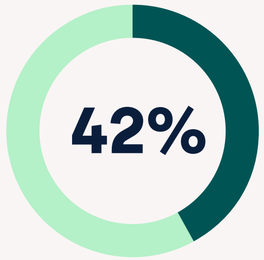
High-value, high-use items like computers, laptops, phones, and home security devices top the consumer protection priority list. But we found that this sentiment wasn't shared across the board. Less than half of consumers say it's important to protect smart home and kitchen appliances for example, while smart TVs and streaming devices came in 6th place. We think it's important that consumers are aware that all smart devices in the connected home should be considered vulnerable.

Will connected home threats become worse with AI?

Some security experts have predicted the rise of AI-powered botnets that could learn and autonomously conduct attacks, mimicking human behavior. And given the security issues that exist in many internet-connected smart appliances, these devices will be an attractive target for these sorts of threats. Nation states, which have the most resources and intelligence to pour into cyber attacks, are certainly looking to compromise IoT vulnerabilities.

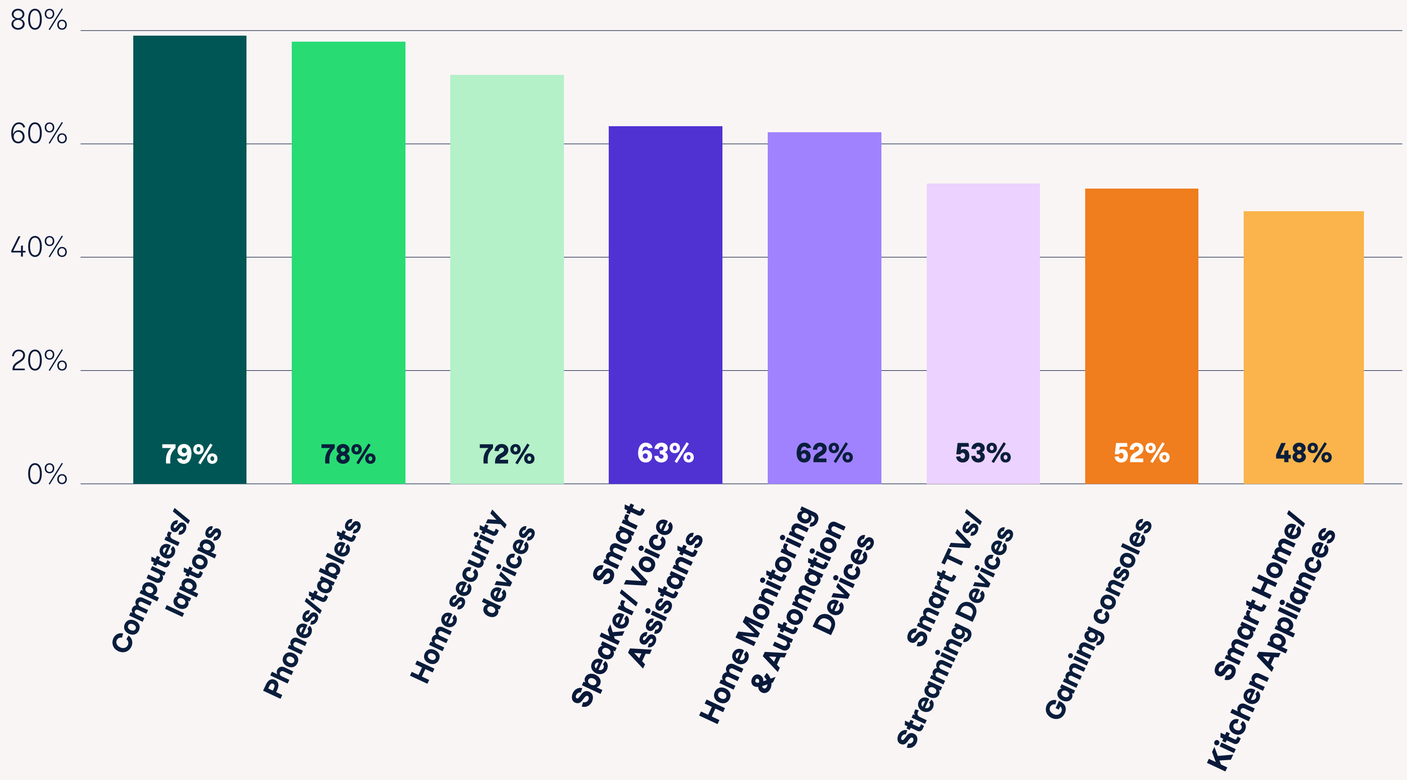


worry that one of their internet connected smart home devices could get infected by a virus/malware or be hacked

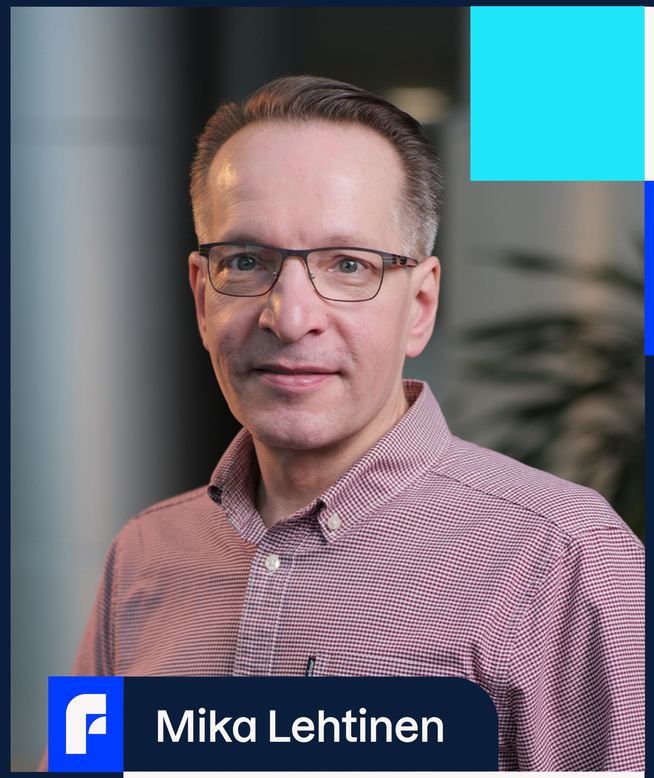


believe smart home device manufacturers are not doing enough to ensure their online security and privacy

% saying it is important to protect selected devices



Source: F-Secure Global Connected Home Survey, 2023



Example: Android TV boxes installed with malware

In late 2023, we commented on findings that suggested devices from hundreds of Android models had been enlisted in a network of zombie devices to commit fraud. **Mika Lehtinen**, F-Secure's Director of Research, explains more below.

These were sold on mainstream sites

"The report identified 77,000 devices with backdoors that open them up to malware installation, but there are probably millions of these boxes sold globally. Affected models were delivered to customers infected with a sophisticated and adaptable malware known as Triada that received active fraud 'modules' as soon as the devices were powered up. What's most significant is that this hardware is being sold through mainstream ecommerce sites like Amazon. The mystery is when the backdoors in the firmware were installed."

Customers were in the dark

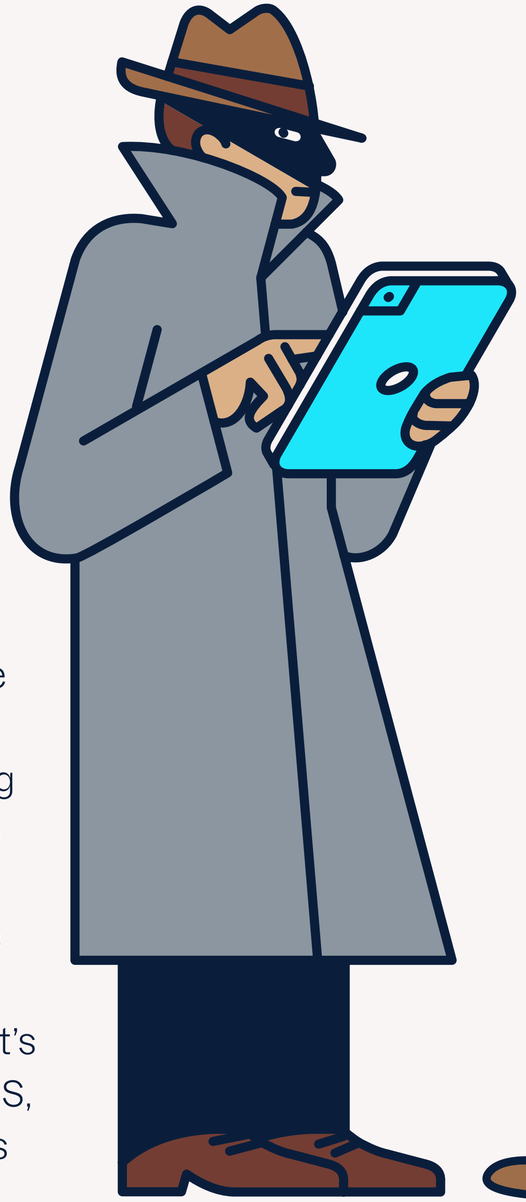
"The ad fraud, fake emails being set up and hijacked proxy, and code installation being carried out by the infected boxes all take place silently. The only sign that your device is participating in a global organized crime botnet may come from slight performance issues. But since these devices are infected from the moment that they're operational, the chances of a customer picking up on this are tiny."

Expert advice for protecting yourself

"When shopping for Android hardware, look closely at recent reviews and try to stick to Play Protect–certified devices. None of the affected boxes were certified by Play Protect."

5 trends and predictions for 2024

Leading experts within F-Secure share their cyber security trends and predictions

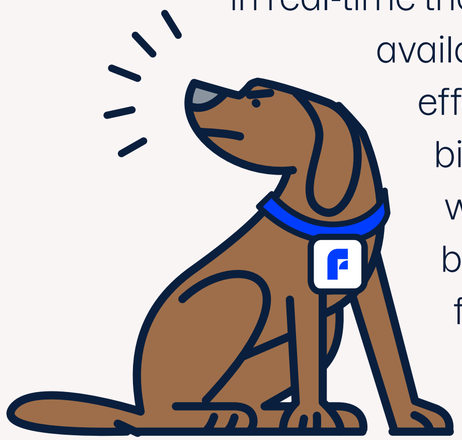


1 SCAMS WILL BE A UNIQUE PROBLEM FOR CONSUMERS

Laura Kankaala
Threat Intelligence Lead

Whether it's on our online banking apps, social media accounts, or dating apps, we're constantly being told to be vigilant against a common threat. Scams. And there's good reason for this – because today, scams pose a unique threat to our online lives. Modern day scamming employs both the manipulation tactics that appeal to our emotional sides with the readily available technology to deliver them, whether that's via email, fake websites, SMS, social media, and more. This makes them a real problem for consumers.

In 2024, this trend will only continue, and we're likely to see a rise in scams that target specific groups of people including those who lead busy lives, are not IT professionals but have to work with computers all day, or haven't implemented the proper measures to protect themselves. We have already witnessed how AI can be leveraged for nefarious purposes by creating fake voices and images, but in 2024 we will begin to see in real-time the true impact of AI and available tools on the effectiveness and capabilities of scams. Finally, we're likely to see scams become the #1 vehicle for consumer-focused cyber attacks.



2 CONSUMERS WILL GET SERIOUS ABOUT PROTECTING AGAINST AI-ENABLED THREATS

Joel Latto
Threat Advisor

If 2023 was the year we started incorporating artificial intelligence into our daily lives, thanks to the adoption of generative AI tools like ChatGPT and DALL·E, then 2024 will be the year we get serious about protecting ourselves against the threats. Before general availability of generative AI, phishing emails, scam SMS messages, and fraudulent websites were much easier to spot because of grammatical errors, spelling mistakes, and generally poor visuals and copy. But now, these threats and scams will become nearly impossible to spot. And AI doesn't only pose a threat to consumers – the use of deepfake and vishing technology makes the threat landscape globally much more complex. This year, I'd expect to see a rise in consumer desire to stay ahead of and protect against AI-enabled threats, both by becoming more vigilant and using the right technology.

3 AI WILL FUEL AN EVOLUTION IN SMART HOME ATTACKS

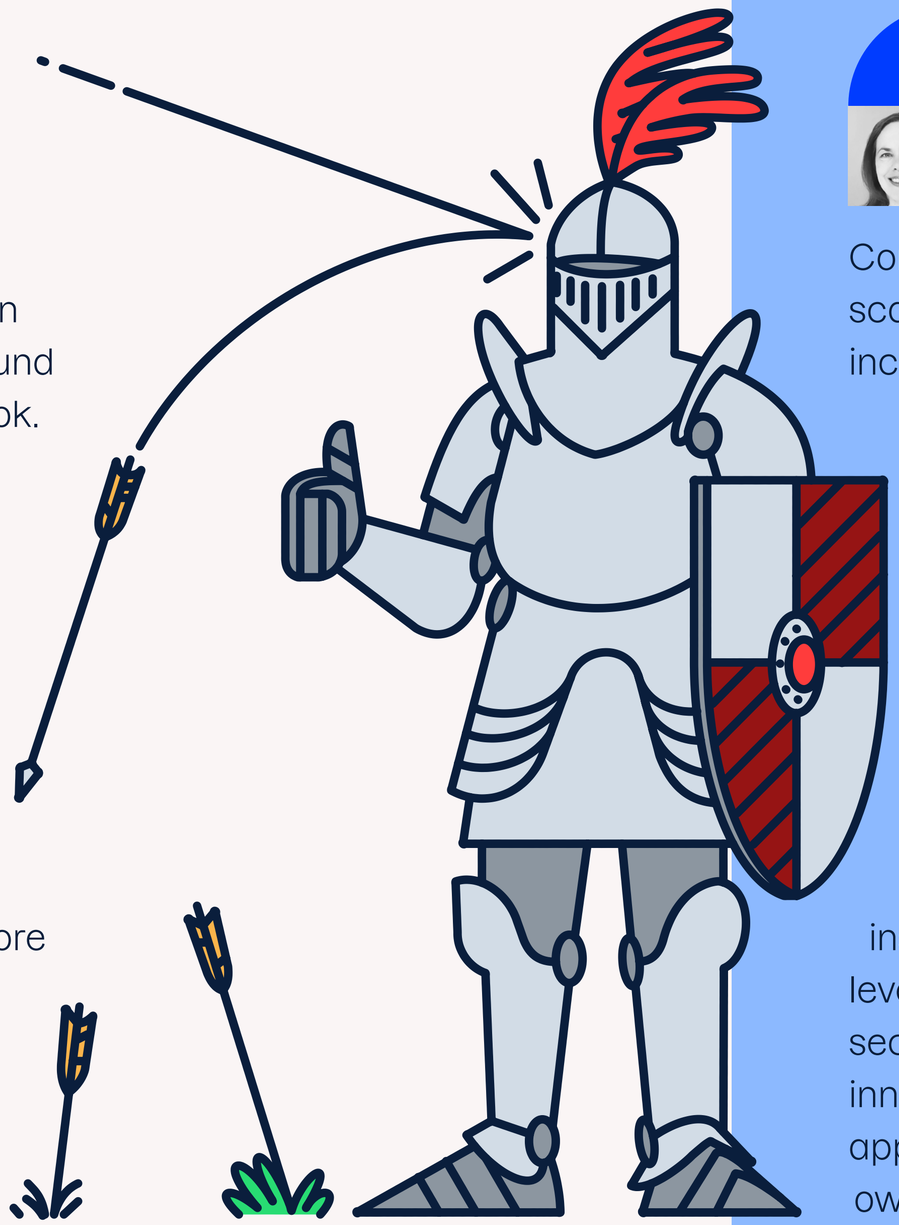
Tom Gaffney
Cyber Security Expert

I expect that this year, we'll see attackers build on the way they have targeted smart home devices previously. AI-enabled products like Amazon's Alexa and Echo are so popular because they make our lives easy. But to help streamline our day to day, they require us to share information, data, and – quite literally – our homes. While the introduction and integration of the newer generative AI tools and capabilities enable these products to better enrich our daily lives, this will also likely increase the level of intimacy we share with these products. As a result, these will unfortunately become increasingly attractive to motivated attackers.

4 ONLINE SHOPPING WILL BECOME RISKIER THANKS TO AI

Yik Han
Researcher

In 2023, we saw a rise in shopping fraud delivered through fake ads on social media, most prominently found on Facebook, Instagram, and TikTok. In 2024, this type of fraudulent advertisement will grow to new heights with the use of generative AI. We are already seeing a rise in the usage of generative AI tools in both legitimate and illegitimate social media advertising, making it hard to differentiate between fake and real ads. Cyber criminals will also create more fake shopping websites and combine them with fake ads to trick victims into making payments and giving out their personal information.



5 CONSUMERS ARE LOOKING FOR A TRUSTED COMPANION

Paula Al Soufi
Director Portfolio Strategy

Consumer trust is plummeting due to an explosion of scams and uncertainties about online security. People are increasingly unsure about who to trust, whether their devices are secure, and how they can protect themselves online. This trend is expected to intensify with the prevalence of deepfakes and AI-generated content.

When it becomes harder to trust anything they see online, consumers turn to their established partners, such as telcos, insurance companies, and banks, seeking a comprehensive security solution for peace of mind online.

This paves the way for an AI Trusted Companion. Telcos, insurance companies, and banks are anticipated to leverage AI for the greater good by combining consumer security solutions with their own AI advancements. This innovative approach aims to deliver a holistic security approach, as these trusted partners rapidly introduce their own AI solutions to combat evolving online challenges."

Sources and methodologies

- GASA Global State of Scams Report 2023, https://www.gasa.org/research
- https://www.forbes.com/advisor/business/ecommerce-statistics/
- F-Secure Online Shopping Survey 2023 (Censuswide), https://company.f-secure.com/en/for-media/experts-warn-shoppers-to-stay-alert-this-holiday-season
- ScamAdviser, https://www.scamadviser.com/
- https://www.f-secure.com/gb-en/online-shopping-checker
- https://www.f-secure.com/gb-en/password-generator
- https://www.f-secure.com/gb-en/articles/what-is-two-factor-authentication
- https://www.w3.org/People/Berners-Lee/WorldWideWeb.html
- https://www.computerworld.com/article/2530462/internet-hits-major-milestone--surpassing-1-billion-monthly-users.html
- https://www.cnbc.com/2023/11/30/chatgpts-one-year-anniversary-how-the-viral-ai-chatbot-has-changed.html
- https://cloud.google.com/learn/artificial-intelligence-vs-machine-learning
- https://knightcolumbia.org/content/understanding-social-media-recommendation-algorithms
- https://en.wikipedia.org/wiki/Universal_translator
- https://krebsonsecurity.com/2023/08/meet-the-brains-behind-the-malware-friendly-ai-chat-service-wormgpt/
- https://www.sciencefocus.com/future-technology/ai-deepfake-scam-calls
- https://www.nytimes.com/2023/08/30/business/voice-deepfakes-bank-scams.html
- https://www.ic3.gov/Media/Y2023/PSA230605
- https://www.f-secure.com/gb-en/articles/staying-ahead-of-cyber-threats-in-the-age-of-ai
- F-Secure Threat Intelligence
- Open Phish, https://openphish.com/
- F-Secured Threats Guide 2023, https://assets.f-secure.com/p/f-secured/annual-threats-guide-2023.pdf
- https://company.f-secure.com/en/for-media/internet-users-still-in-the-dark-about-the-dark-web
- https://www.f-secure.com/en/identity-theft-checker
- https://blog.google/technology/safety-security/passkeys-default-google-accounts/
- F-Secure Connected Home Whitepaper, https://assets.f-secure.com/p/partners/20230912-connected-home-whitepaper.pdf
- https://twitter.com/malwrhunterteam/status/1618721906114572290/photo/1
- https://blog.f-secure.com/infostealers-and-macos/
- https://darktrace.com/blog/vipersoftx-how-darktrace-uncovered-a-venomous-intrusion
- https://fidoalliance.org/members/
- https://www.passkeys.io/who-supports-passkeys
- www.statista.com
- F-Secure Global Connected Home Survey, 2023
- https://github.com/DesktopECHO/T95-H616-Malware (Daniel Milisic)
- https://www.wired.com/story/android-tv-streaming-boxes-china-backdoor/
- F-Alert October 2023

F-Secure Online Shopping Survey 2023 was conducted by Censuswide, among a sample of 4,001 consumers, aged 16+, across the UK, Germany, and Finland. (2,000, 1,001 and 1,000 nationally representative respondents respectively) The data was collected between 11.10.2023 – 23.10.2023. Censuswide abides by and employs members of the Market Research Society and follows the MRS code of conduct which is based on the ESOMAR principles. The UK sample was nationally representative of age, gender and region. The Germany and Finland samples were nationally representative of age and gender. Extrapolations based on amount of money lost to scams at Christmas (3%) or in the last 12 months (5%), have had outliers taken out to validate the results.

F-Secure Global Connected Home Survey was undertaken in June 2023. The total number of respondents was 4400. Data in charts selected from 11 countries: Brazil, Germany, Finland, France, Italy, Japan, Netherlands, Norway, Sweden, United Kingdom, United States. (N = 400/country, age 25-74 years).

F-Secure ID Theft Survey 2023 (Censuswide) The survey commissioned by F-Secure (2023), four countries (United Kingdom, Finland, Germany, Sweden), sample size 2000/UK and 1000/Finland, Sweden, Germany, total 5000 respondents.

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 200 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.com today.

F-Secure®