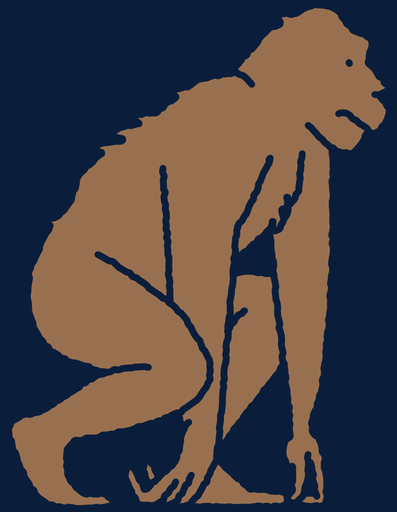
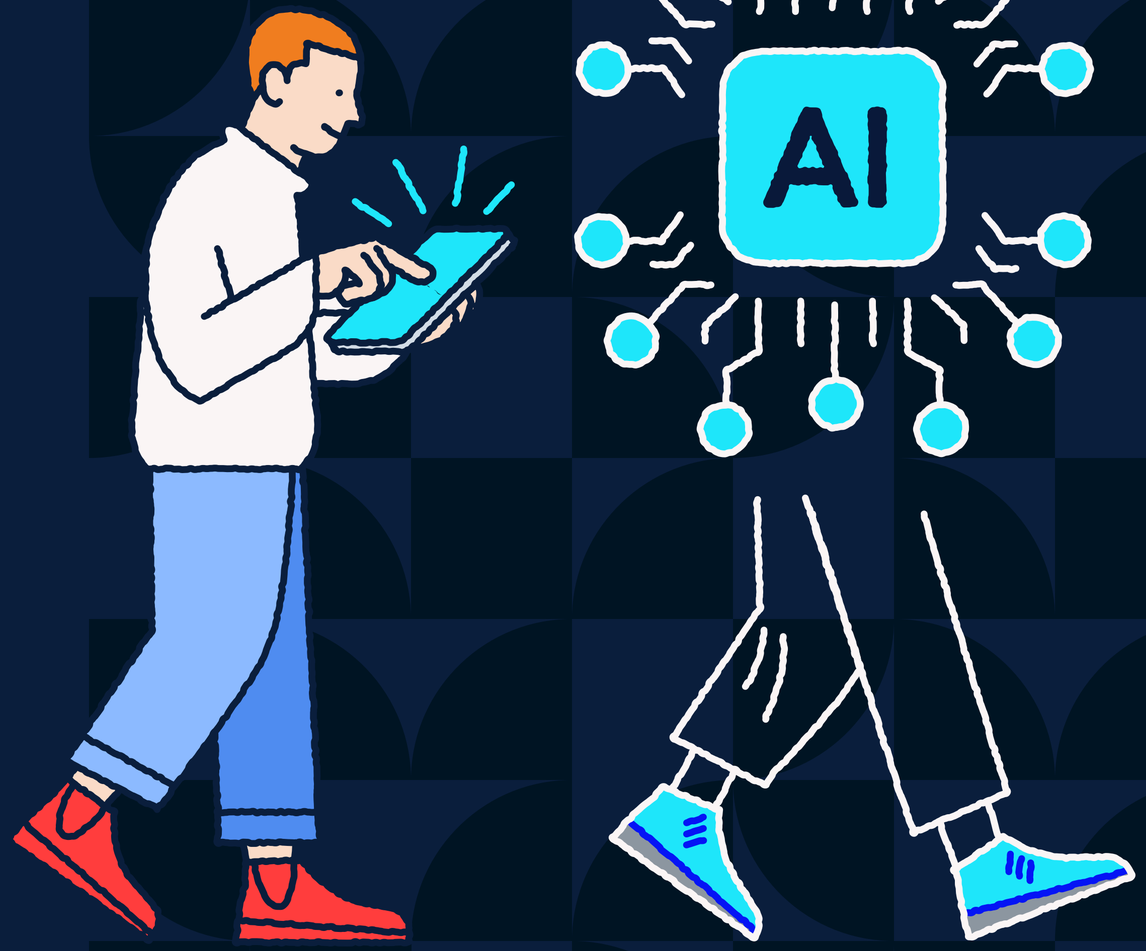
F-Alert

Monthly threat updates from

F-Secure

2023 Wrap-up





F-Secure

Discover the latest threat updates. Packed with insights from the experts at F-Secure. Delivered every month.

See how scams became the most common form of cyber crime. Find out how consumers are targeted through small businesses. And discover how AI is already creating a crisis for young girls. In this supersized year-end edition of F-Alert, we look back at the biggest cyber security news and forward to see how the New Year could transform both the internet and reality itself.

PREDICTION

The deepfake crisis is here

Girls are already dealing with the peril of fake AI nudes and adults need to catch up.

Laura Kankaala
Threat Intelligence Lead
Helsinki, Finland

expert tip

Victims can try to contact local law enforcement. In some, but too few, countries and states, spreading deepfakes is a crime. If it isn't, contact your local lawmakers to make it one.

"Deepfakes are a technology destined for misuse."

You may not have heard of apps that can put someone's face on the body of an actor in a pornographic movie or "undress" anyone using AI. But your kids probably have.

Deepfakes — images or videos where one face is replaced with another — have been around for years. But as part of the generative AI revolution, they keep getting more realistic. And society is not prepared for the consequences.

The cost of living online

Deepfakes are a technology destined for misuse. They could be used for political attacks, as a part of scams, and to smear the reputations of business leaders — or pretty much anyone.

But the best example of what a worst-case version of the future will look like comes from how these forgeries are being used against girls right now. The new school year has brought multiple incidents of fake nude photos of students being spread widely, often leaving officials unsure how to respond.

The rise of AI seems to have made the public more aware of how easy-to-use this technology is. But what perpetrators are also taking advantage of is how much of is our lives are online. There is likely an abundance of images, videos, and audio of you, strewn across multiple social networks, especially if you've grown up in the post-Facebook era. Any of that could be transposed into other media.

Taking digital abuse seriously

AI itself will be used to catch at least some of the deepfaked sexual material. But these tools are only helpful if online platforms take responsibility for material submitted by their users.

And the platform is where you should start if you are depicted in a deepfake being spread online. Some of the biggest online service providers are also part of the Stop Non-Consensual Intimate Image Abuse initiative, through which you can try to get the content removed.

But removal isn't enough. Openness about the trauma potentially caused by digital abuse is crucial. Talking to someone you can trust—whether it's a support group for victims of sexual abuse or a loved one—is key to taking the real distress caused by these fake videos seriously.

EU law aims for an open internet

The EU will begin enforcing the Digital Markets Act for fairer competition next March.

The Digital Markets Act (DMA) has the potential to be one of the most transformative laws ever to reshape our digital lives. That's why we asked Miina Hiilloskivi-Knox, Legal Counsel at F-Secure, to give us an overview of this "centerpiece" of the regulations that make up the EU's 2020 data strategy to create a "fair and open" internet.

Meet the gatekeepers

A key step since the law became applicable in May of 2023 has been identifying the gatekeepers that provide "core platform services," like search engines, operating systems, and online advertising systems.

"The EU Commission designated Alphabet, Meta, Apple, Amazon, ByteDance, and Microsoft as gatekeepers in September 2023," Miina said.

These companies have until March 2024 to ensure that their products – which include Google Maps, YouTube, Instagram, Apple AppStore, TikTok, and Windows PC OS – comply with the 22 new obligations defined by the regulation.

"As these gatekeepers operate globally, we'll most likely see changes in the ways these companies operate across the world."

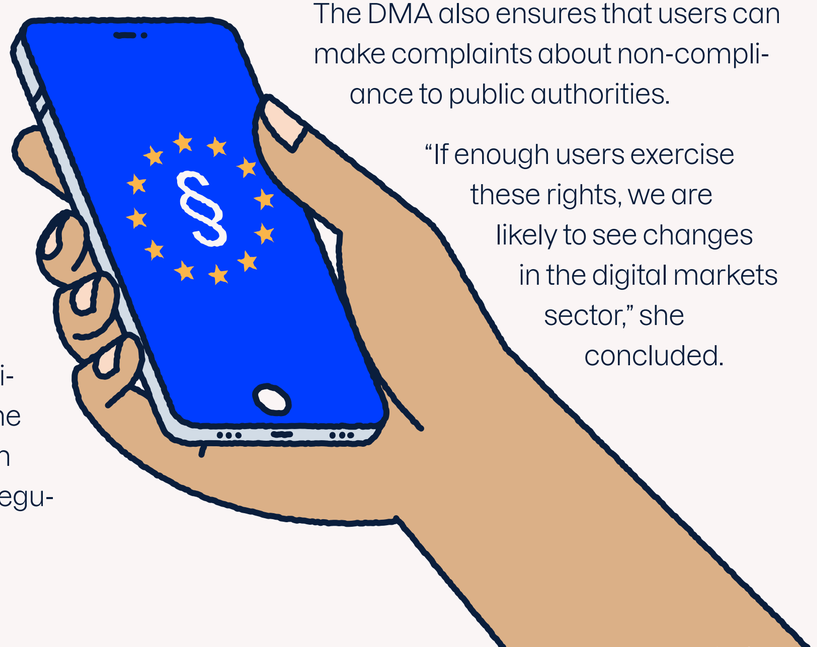
Regulating real power

Miina noted that the DMA is significant in that it is the first EU regulation that focuses on regulating the power of the largest digital platforms.

"Gatekeepers cannot show preferential treatment to its own offerings," she said. "The DMA also prohibits gatekeepers from tracking users outside of the gatekeeper's core platform for marketing purposes unless the user has given explicit consent."

The DMA also ensures that users can make complaints about non-compliance to public authorities.

"If enough users exercise these rights, we are likely to see changes in the digital markets sector," she concluded.



Miina Hiilloskivi-Knox
Legal Counsel
Helsinki, Finland

expert tip

The Digital Markets Act does not impose new security obligations on gatekeepers, so platform users should remain vigilant online.

"We'll most likely see changes in the ways these companies operate across the world."

Trending Scam

Failed delivery trickery

WHAT:
Failed delivery scams that play on expectations of unexpected gifts arriving for the holiday season have been around for years. What's newer is that these scams are increasingly likely to arrive via SMS rather than email. And now they often include the twist that a delivery driver messages to say s/he cannot find your house.

HOW:
A message arrives either through text or email from a major delivery company that says a driver was unable to deliver a package to your residence. Often the message comes with a link claiming to provide tracking information. That link likely leads to an infostealer that will suck up your credentials.

PREPARE:
The delivery services are aware of these scams. As a result, they will likely never contact you over email or text to inform you of a failed delivery, especially during the holiday season. You can safely ignore all these messages. If you cannot resist the urge to find out more about a delivery you hoped to receive, contact the shipper without clicking on any link you've been sent.

Breach that matters

LinkedIn

WHY IT MATTERS:
LinkedIn is the only major social network that has been around two decades and remains a crucial platform for individuals and businesses around the globe. In November of 2022, criminals claimed to have personally identifiable information of half a billion users of the site and released 2 million records as proof. Nearly 15 million stolen records have been confirmed.

BREACHED DATA:
The data includes emails, usernames, phone numbers, and other personal information that can be used to identify or target site members.

WHAT SHOULD YOU DO:
Active LinkedIn users typically receive multiple emails from the site weekly, if not daily. For the time being, everyone should avoid all emails claiming to be from the site and refuse to click any links inside these messages. Go directly to the site to follow up on any email notifications you receive.

Is your data being exposed online?
Check with our **F-Secure Identity Theft Checker!**

PREDICTION

Small businesses' data targeted

Crime groups will increasingly sell access to breached smaller businesses so attackers can scam consumers.

Ash Shatrieh
Threat Intelligence Researcher
Helsinki, Finland

expert tip

Be mindful of fraudulent communications even from familiar names, as hackers now often use credible businesses as a disguise for phishing attacks.

“The consumer data stored by SMBs has become a hot commodity for cyber criminals.”

For much of the last decade, the big money in cyber crime came from ransomware attacks against big organizations. That threat persists. But criminals will likely shift their focus towards small and medium-sized business (SMB). And the consequences for consumers will be huge.

Crimes of convenience

The use of Software-as-a-Service (SaaS) technology for core business functions continues to integrate SMBs into the global supply chain. And because any vulnerability potentially offers attackers a way into other organizations in the chain, criminals often take advantage of the weaker security measures employed by SMBs.

Meanwhile, the cyber crime black market has mirrored innovations in legitimate services. Cyber crime-as-a-service makes campaigns easier and cheaper to carry out.

Smaller businesses already deal with more breaches than their larger counterparts. This trend is likely to escalate as big cyber crime groups focus on selling hacked access to attackers, who will then be able to fully exploit the stolen data to craft hyper-personalized scams, greatly increasing the success rate of their schemes. And that’s just the beginning.

A perfect storm

Attackers can also exploit the social media or email accounts of compromised businesses. This gives them the ability to weaponize the company’s hard-won credibility, creating a perfect storm of deception that can be used to spread disinformation or cyber crime campaigns.

But the storm likely won’t stop there. Websites have been infected to skim credit card numbers for years. But we expect to see more attackers embedding other malicious scripts into SMB websites to mine cryptocurrency or redirect users to fake updates. As a result, consumers may unwittingly fall victim to scams that operate in plain sight.

Google's AI checks itself

Bard now allows users to "Google" the chatbot's answers to see if it's making stuff up.

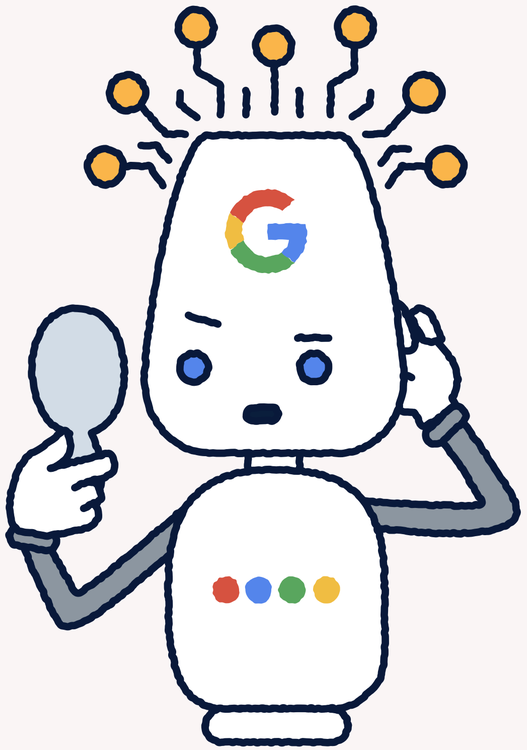
One of the most often cited concerns about AI chatbots is that the answers they generate may have been "hallucinated" and not actually based in facts. Two lawyers from New York learned this lesson the hard way when they were sanctioned for submitting a legal brief that included citations of six cases that were invented by ChatGPT.

Hoping to avoid this kind of confusion, Google has added a new feature to its "conversational AI tool" Bard allowing users to "double check" the facts of an AI response with a Google search.

A feedback loop of bad information

"Generative models, while powerful and rather accurate, are not infallible," said Khalid Alnajjar, a Threat Data Researcher at F-Secure. "They're trained on vast quantities of online data, absorbing, and replicating the patterns they find."

Khalid noted that the problems with AI-generated content could easily increase as "future versions of these models may learn more from their own creations." Additionally, these models will inevitably be fed by misinformation and purposely harmful disinformation spread by humans.



"This could create a feedback loop of bad information unless mechanisms are implemented to prevent it."

A long journey

Khalid called Bard AI's "Google it" feature a significant advancement in this field but warned that it's just the beginning of a long journey to ensuring generative AI produces reliable text.

"The fact checking is conducted by a Google search that references whether the system generated is real or not," he concluded. "This approach does not come without problems as Bard AI might well be checking its output against fake news stories."

Khalid Alnajjar
Threat Data Researcher
Helsinki, Finland

expert tip

Always approach AI-generated content with a degree of skepticism. When AI provides sources to back up its statements, don't just take them at face value — check their credibility.

"Generative models, while powerful and rather accurate, are not infallible."

SCAMS are the new BLACK

The cyber crime you're most likely to face is all about fooling you into making one bad choice.

Scams are a trillion-dollar business, infecting more than 1 out of 4 people on earth.*

Scams are multichannel, explained Joel Latto, Threat Advisor at F-Secure.

"That means they can happen to you both online and off," he said.

But if you're going to fall victim to a cyber crime today, it's most likely going to happen through your phone.

"And rather than infecting you with a malicious file, criminals are most likely to get to you using a text message or a phone call," he said. "And they're just trying to find some way to get you to look at that screen and make one bad click."

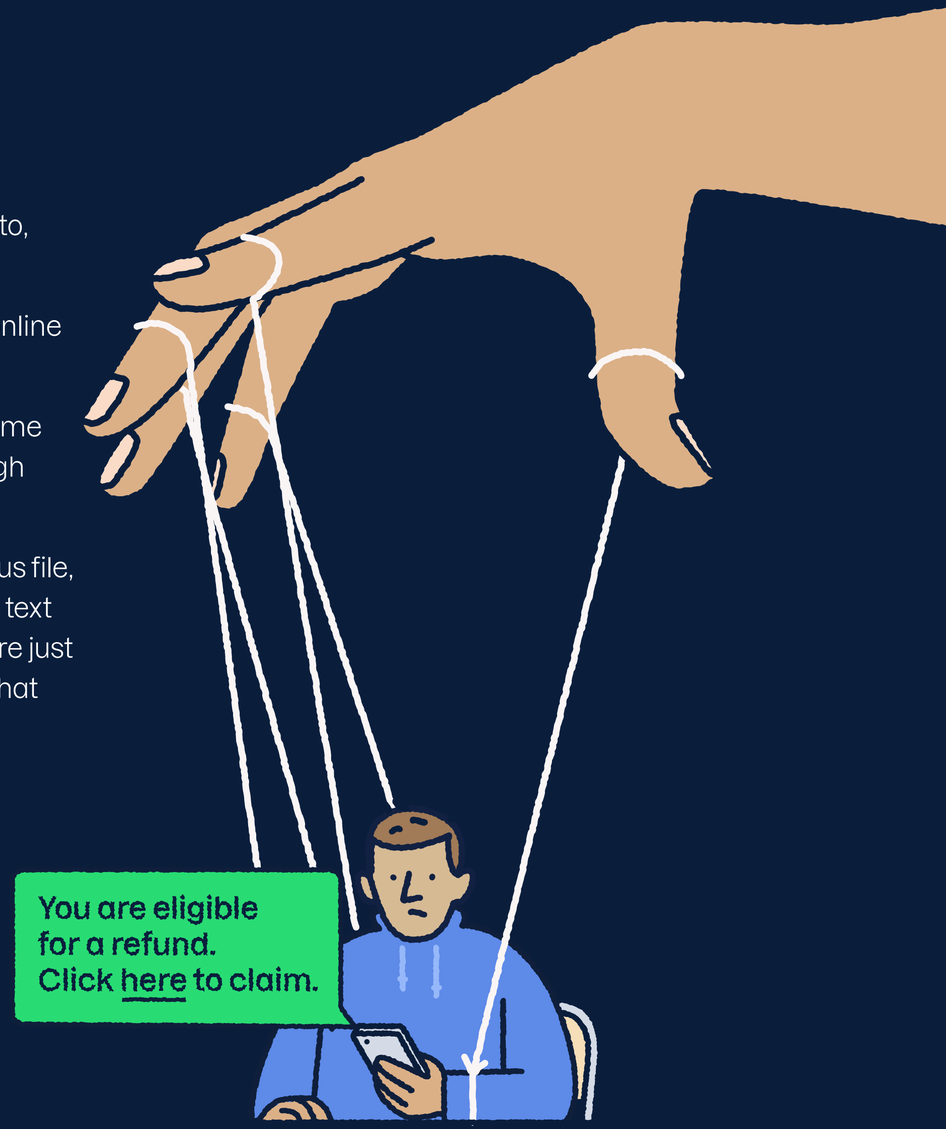
Most common forms of cyber crime**

12% SMS scam

11% Call fraud

8% Malware and viruses

6% Credit card fraud



*Source: The Global State of Scams – 2023, ScamAdviser ** Source: F-Secure Consumer Market Research June 2023, 11 countries (Brazil, Finland, France, Germany, Italy, Japan, The Netherlands, Norway, Sweden, UK and USA), n=4400

Joel Latto
Threat Advisor
Helsinki, Finland

expert tip

"Everyone makes a bad click eventually. That's why you need a high-quality security solution like F-Secure Total that includes Browsing Protection."

Criminals use whatever topic is trending to get your attention.

And AI chatbots are only making it easier to localize scams.

"Recently I spotted examples of one Facebook scam in Swedish, Hungarian, French, and German, where previously I had seen it almost exclusively being delivered in English," he said.

Malware is how cyber criminals get into your devices. Scams are how they get into your brains. And fooling people can be both a quantity and a quality game.

"An example of a large-scale scam would be a spam campaign with fake Facebook ads aimed at large audiences," said Joel. "But targeted scamming can be just as big of a threat and in that case, the criminal may have researched your online life before it even begins."

PREDICTION

AI will be bigger than the internet

Anyone who ignores artificial intelligence will suffer the same fate as those who ignored the internet.

Mikko Hyppönen
Principal Research Advisor
Helsinki, Finland

expert tip

Try uploading a long PDF – in any language – to Claude.ai or ChatGPT and asking for a summary. I think you'll be impressed. I tried this with several papers I wrote, and I certainly was.

"We will be remembered as the first people who had access to AI."

The internet erased borders. It triggered a revolution so transformative that I wrote in my book If It's Smart, It's Vulnerable, which was published in the summer of 2022, that we will be remembered as the first people who went online. I was wrong.

We will be remembered as the first people who had access to AI.

Three revolutions at once

The internet was just the first of three revolutions happening roughly at the same time, which brought us to the AI explosion we're experiencing now.

Bringing nearly every computer online helped turn all content that existed on paper into data. The second revolution was a part of the first and it gave us the ability to store all that data. We call this "the cloud." And the third revolution is probably in your pocket now. It's not your phone itself. It's the computing power in it. A typical smartphone from 2023 would have been one of the top 500 supercomputers on the planet just 20 years ago.

The result is that we can now teach computers to create images that aren't limited by creativity, and we have large language models that can speak all human languages. Within a decade or so, we'll be able to pick any actor we want to star in whatever movie we want to watch on Netflix. Eventually, AI could also be used to cure cancer, solve climate change, and rewrite its own code to continually improve itself.

The second-most intelligent species

What does this mean for us? Is it a smart decision to intentionally make ourselves the second-most intelligent species on the planet? How can human beings, with our average 100 IQ-intelligence, project that superhuman AIs with a billion IQ will behave?

What we can do now is think about how AI can be used, and misused. Because if you don't, you can be sure that your competitors, and the scammers who may use AI to target you, will.

Booking.com ecosystem targeted

Fake confirmations show how difficult it is to secure a network of millions of hotels and private hosts.

Act fast. Send us your credit card information. Or you will lose your reservation.

That was the message inside "confirmation" emails recently sent to numerous Booking.com customers. The company denied a hack of its systems and suggested that partner hotels' systems had been breached. But that's little consolation for customers who were told by their company that their credit card details may have been compromised.

Trust can be exploited

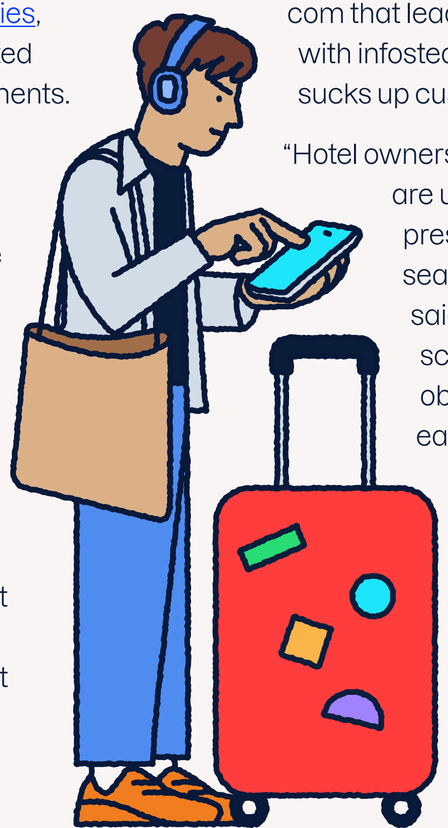
"Booking scamming is not new but it is getting more advanced," said Hoai Duc Nguyen, a Threat Protection Researcher at F-Secure. "But this example shows how difficult it is to secure an industry where multiple platforms are renting rooms from both hotels and private owners."

Booking.com is one of the most popular travel apps in the world. It offers lodging reservation services for nearly 3 million properties, including 2.3 million affiliated private homes and apartments. Attackers pulled off these attacks by exploiting the trust between customers and messages sent by the booking platform and the customer's fear of missing out on travel plans.

High season for scammers

"Private hosts are the most vulnerable to scamming and phishing as they aren't often trained against cyberattacks," Hoai Duc added.

Researchers have identified phishing attacks targeting private hosts and hotels that work with Booking.com that lead to an infection with infostealer malware that sucks up customer data.



"Hotel owners and hosts are under extreme pressure during high season," Hoai Duc said. "While these scams may seem obvious, it's much easier to be fooled when you're dealing with hundreds-to-thousands of bookings."

Hoai Duc Nguyen
Threat Protection Researcher
Helsinki, Finland

expert tip

Think twice when you receive an unexpected message with strong emotion, a warning in which money is involved—even when that message is from a trustworthy partner.

"Booking scamming is not new but it is getting more advanced."

PREDICTION

AI will boost shopping scams

Fake ads that push luxury items will reach new heights thanks to AI-generated images and text.

Yik Han
Researcher
Kuala Lumpur, Malaysia

expert tip

When submitting credit card details, make sure the payment processor is legitimate. Familiarize yourself with common checkout pages, like those of Amazon, Shopify, and Stripe.

“Generative AI tools will help scammers create more convincing captions and shockingly detailed images.”

This year saw a dramatic rise in shopping frauds delivered through fake and fraudulent advertisements for luxury goods on social media, most prominently found on Facebook, Instagram, and Tik Tok. In 2024, these bad ads will likely evolve into new heights with the use of rapidly advancing generative artificial intelligence (AI).

Artificial intelligence, real scams

Billions of people around the globe have used AI chatbots to generate text and images since the release of ChatGPT brought the technology into the mainstream in late 2021. Advances in generative artificial intelligence have been persistent and extensive, as giant tech competitors including Google and Microsoft seek advantage in this rapidly expanding space.

And while these bots automate numerous tasks, they are also frequently misused. In April of 2023, Europol noted that large language models (LLMs) like the one that powers ChatGPT could be exploited by criminals for fraud, disinformation, and cyber crime, noting specifically that LLMs are an “extremely useful tool for phishing purposes.”

Numerous benefits, but not perfection

Generative AI tools will help scammers create more convincing captions and shockingly detailed images on their fake advertisements. F-Secure has already seen a rise in the usage of generative AI tools in both legitimate and illegitimate social media advertising posts.

Cybercriminals are also likely to create more fake shopping websites and combine them with malvertising to trick victims into handing over their credit card numbers. With the help of generative AI to instantly aid the construction of entire ecommerce experiences and help craft professional marketing messages, these fraud sites will become even more difficult to be detected.

F-Awards

For Excellence in Protecting Digital Moments

Making every digital moment secured is a team effort. So as 2023 closes, we wanted to honor cyber security breakthroughs that have made us all a little safer this year.

Best Security Innovation: Passkeys

Apple, Amazon, and Microsoft have all implemented this new authentication method. But this fall brought a breakthrough for this technology designed to be fast, safe, and easy-to-remember. Google made passkeys default on all personal accounts. That should mean that the death of passwords is imminent. Good riddance.

Best Takedown: Genesis Market

The numbers are massive. Law enforcement agencies from 17 countries making 119 arrests. More than 1. 5 million computers compromised. Over 80 million account credentials for sale. The takedown of the Genesis Market in April set a new standard for international cooperation to close a marketplace selling stolen credentials. Well done.

Best Scam Prevention: Google Verification

Google calls it BIMI, Brand Indicators for Message Identification. It's been around since 2021, but this year the company added a blue checkmark in your Gmail that indicates an email comes from the company that claims to have sent it. This won't eliminate all phishing scams. But it should help.

Best Unintended Consequence: X charges for SMS 2FA

X (formerly Twitter) announced in February that it would charge for two-factor authentication (2FA) using SMS messages. While this move would weaken the account security of those who turned off the feature, it also pushed users to adopt a free authenticator app, a more secure option to lock down an account. If you haven't, drop all those SMS 2FA codes and use an app!

Best Simple Solution: Online Shopping Checker

With modern web tools and AI, creating a legitimate feeling webstore only takes minutes. So why wouldn't criminals set up a fake store and reap the rewards? Consumers finally have a way to easily see if the stores they've landed on are legitimate. Online Shopping Checker instantly checks a shop's reputation for free. And the same technology is now included in F-Secure Total's Browsing Protection. Try it!

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