F-Alert

SCAM EDITION

Monthly threat updates from

F-Secure

April 2024

F-Secure

Scam Wars: The Rise of AI-Driven Deception

With severe financial losses to fraud reported worldwide, we deep-dive into the ever-increasing onslaught of online scams and explore the latest threats informed by our experts:

- Scammers steal faces in AI attack
- Exposing online scams: an epidemic
- Are deepfakes blurring reality?
- New hub spotlights the latest scam tricks
- 'Click farms' scam algorithms
- Old scam, new packaging
- 2FA leak exposes social media users
- ChatGPT: is your data safe?

Scammers steal faces in AI attack

A new trojan bypasses biometrics to steal from bank accounts.

Goldpickaxe, a sophisticated new malware developed by Chinese threat actor GoldFactory, has been targeting biometric data to bypass banking security and steal money in Thailand and Vietnam.

Ash Shatrieh, Threat Intelligence Researcher at F-Secure, investigates: “Using a combination of social engineering and fake apps, Goldpickaxe gathers facial biometrics, text messages, and video recordings to create deepfakes that grant attackers access to victims’ bank accounts.”

Step 1: Luring victims

The attacker sends phishing messages directing victims to a communications app and may call them impersonating government entities to gain their trust. The goal is to get them to download a fake app disguised as a real service, like the Thai ‘Digital Pension’ app.

Step 2: Distributing links

The malware infects devices through a counterfeit website that closely resembles the official Play Store (Android) or by convincing the victim to download Mobile Device Management profiles to remotely configure devices or sideload apps (iOS).

Step 3: Obtaining biometrics

After installing the malware, it prompts victims to provide their ID documents and record a video as a 'confirmation method,' which is then used to create deepfakes. When capturing the video, instructions such as ‘blink’, ‘smile’, and ‘tilt your face’ are given to the victim on screen to create a comprehensive facial biometric profile.

Step 4: Bypassing security

The malware is also capable of intercepting SMS to gain access to verification codes used in two-factor authentication. Furthermore, it can proxy the threat actor's network traffic through the victim's phone. This enables attackers to route traffic to banking apps while evading security measures on a victim's carrier, geographical location, or device ID.

How to protect yourself

“It’s important to clarify that this malware does not bypass iOS or Android's biometric security features,” explains Shatrieh. “However, using an online security solution is the best way to protect yourself.”

“F-Secure Total blocks all the currently identified indicators of compromise and variants for this threat on Android devices, and on iOS devices when F-Secure VPN is active. F-Secure VPN blocks communications with different command and control servers deployed by the threat actor as well.”

Ash Shatrieh

Threat Intelligence Researcher

Helsinki, Finland

expert tip

Staying informed, exercising caution when downloading apps, and making use of security solutions are crucial for protecting yourself in an evolving threat landscape targeting biometrics.

Mobile Device Management (MDM) is used to control, secure, and enforce policies on a device.

EXPOSED

Online scams: an epidemic

The Global Anti-Scam Alliance (GASA) warns of an international emergency.

The news is rife with scams. A quick Google search will bring you hundreds of thousands of articles posted mere hours apart. Crypto scams. Romance scams. Even government imposter scams. With people all over the world affected by fraud, here are some key insights into the global state of scams.

$1.026 trillion

stolen by scammers

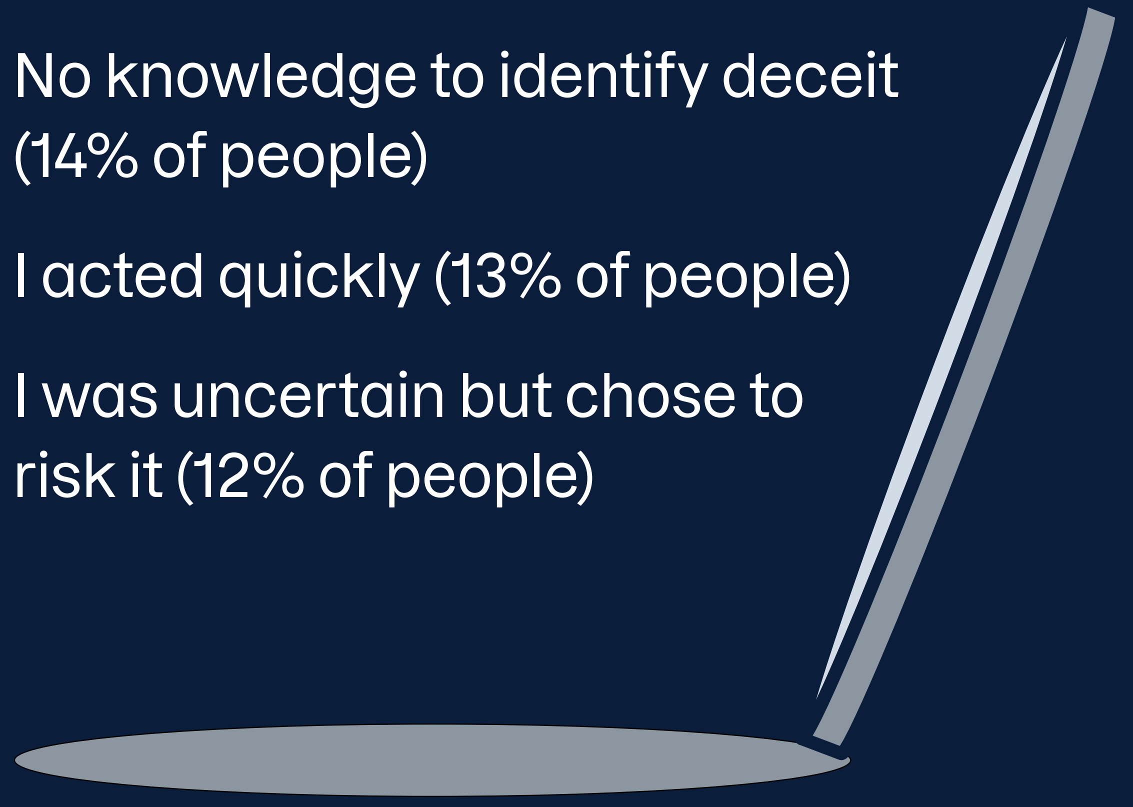
1 in 4 people

defrauded globally

...in just one year.

Why do we fall for scams?

1. An attractive offer was made (25% of people)
2. Deceit was not identified (17% of people)
3. No knowledge to identify deceit (14% of people)
4. I acted quickly (13% of people)
5. I was uncertain but chose to risk it (12% of people)



Source: GASA The Global State of Scams 2023

Which countries are affected the most?

Kenya – victims were scammed almost 3 times each

Brazil – 81% encountered a scam at least once per month

South Africa – 59% received scam attempts via Gmail

Argentina – 30% fell victim to identity theft

Malaysia – 57% aren't confident in recognizing scams

Hong Kong – scams have grown in frequency by 71%

USA – 3 in 4 Americans experience a scam monthly

Today, almost everything we do is digital – from paying bills and banking online to online shopping and dating. And scammers have capitalized on this, using a variety of tactics to trick people. These include:

- Emotional manipulation
- Fearmongering
- Time pressure
- Gaining their trust

Top 5 platforms used by scammers:

1. Facebook
2. WhatsApp
3. Gmail
4. Instagram
5. Telegram

Favorite channels used by scammers:

1. Phone calls (61%)
2. Text messages (58%)
3. Email (40%)
4. Instant messaging (39%)
5. Social media posting (34%)

How can you avoid online scams?

By taking care of your cyber hygiene and remaining vigilant online, it's possible to dodge interactions with scammers. Tips from our experts include:

1. Use our free tools to check the legitimacy of online shops, text messages, and more.
2. Browse our articles to stay up to date with the latest scams and expert advice.
3. Make protecting your digital life effortless with a cyber security solution such as F-Secure Total.

Source: GASA The Global State of Scams 2023

Are deepfakes blurring reality?

Seeing is no longer believing – scammers are using AI for financial gain.

A worker at a multinational firm in Hong Kong was recently the target of an advanced AI scam weaponizing deepfake technology to trick him into transferring an eye-watering $25 million to who he believed was the company's CFO.

Joel Latto, Threat Advisor at F-Secure, explores this story and provides expert insights and expectations about the unnerving topic of deepfakes.

An elaborate plan of attack

The ploy started when the worker received a message claiming to be from the company's UK-based CFO asking for a secret transaction to be carried out. Although initially suspicious, he put his doubts aside after a video meeting with what seemed like other company employees – but they were all deepfake recreations – and he then sent $200 million Hong Kong dollars ($25.6 million USD) to the scammers.

Are deepfakes the future?

"Scamming with real-time deepfakes is not yet a threat to the masses due to the amount of work required by criminals. It is, however, a threat that will more likely impact business leaders and other high-profile people, as seen in this case" explains Latto.

"Pre-recorded deepfakes are more prevalently being used to give a new spin to old scams that could target just about anyone. For example, the "Hi mum" SMS scam has been upgraded to include a follow-up call using deepfaked audio of a person's child."

While we're not there yet, it's just a matter of time before real-time deepfakes become easy enough for criminals to deploy en masse – which will make deepfakes more of a threat to consumers.

Prepare for every eventuality

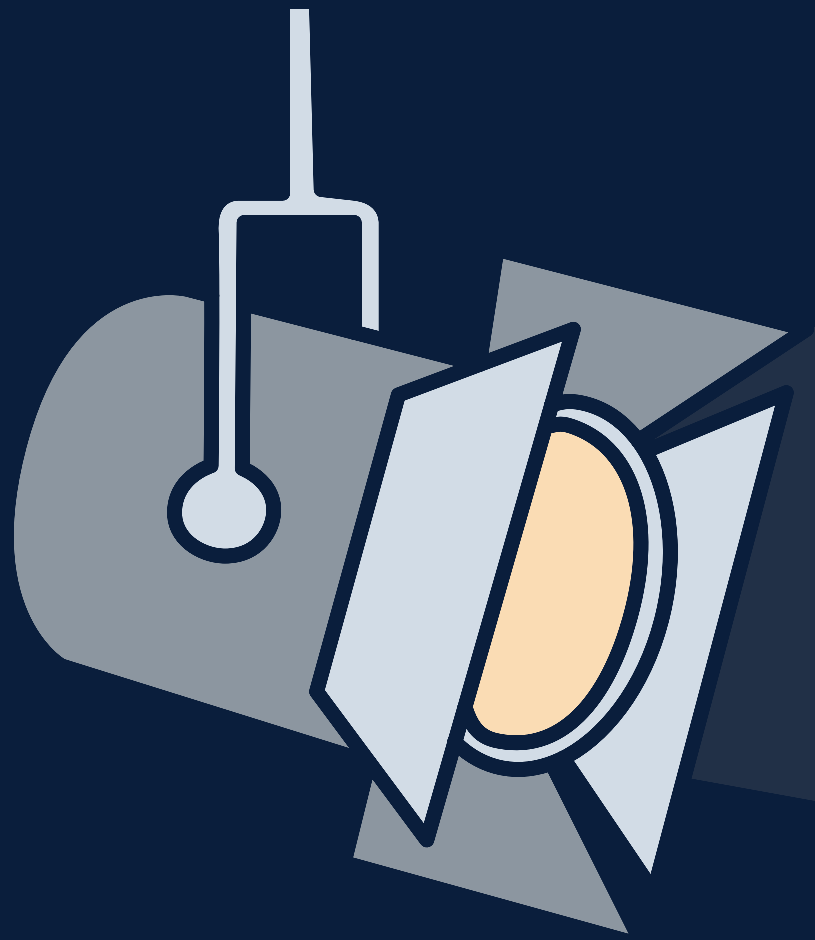
According to Latto: "A good preventative measure is to agree on a code phrase with your family. Something that can be used to verify that you're really talking with the person they're claiming to be."

Joel Latto
Threat Advisor
Helsinki, Finland

expert tip

If you receive a phone call from someone you know and they ask you to do something out of the ordinary, hang up and call the number you have saved for them to verify the authenticity of the request.

> **"Pre-recorded deepfakes are being used to give a new spin to old scams."**



New hub spotlights the latest scam tricks

Discover everything you need to stop scammers in their tracks from the leader in scam protection.

From AI-enhanced romance scams to online banking fraud, find out from F-Secure experts how to identify, avoid, and protect yourself against new developments in scamming.

Assess online threats with the F-Secure Scamometer

Use our free Scamometer to instantly gauge which online activities are most at risk from sneaky scammer attacks.

Try it now

The latest online scam in our spotlight... Imposter scams

Explore our Scam Protection Hub

Laura Kankaala
Threat Intelligence Lead
Helsinki, Finland

expert tip

Look beyond the slick presentation and question your sources: what credibility do they have?

> **“The setup is simple: hundreds of devices swarming with fake profiles.”**

'Click farms' scam algorithms

Operations are artificially generating engagement on social media.

Vietnam is known for its rice farms. But there’s a different type of farm operating from shadowy basements around the country that’s attracting the attention of cyber sleuths: click farms.

Cultivating likes and comments

Social media can be a marketing goldmine. But not all that glitters is gold. Instead, shady enterprises around Asia built to boost social media engagement could be hiding behind a brand’s popular profile.

“Enticed by low labor and energy costs, these operations artificially manipulate social media algorithms with fake likes, comments and shares,” explains Laura Kankaala, Threat Intelligence Lead at F-Secure. “The setup is simple: hundreds of devices swarming with fake profiles. They may even be wired together in a ‘box farm’ and linked to a computer interface.”

One worker – 10,000 clicks

If you’re imagining a mafia-type mastermind behind these operations, you’d probably be mistaken. They’re in fact more likely to be a family-run business or a young startup-type company. One ‘farmer’ boosts engagement on Facebook, while another looks after YouTube – watching videos on repeat.

“Sinisterly, click farms are also being used to spread fake news and political disinformation,” says Kankaala. “For example, during the 2016 US presidential election an operation in Macedonia was found to have created more than 100 websites spreading fake news that favored Donald Trump.”

Knowledge is power

Social media is practically inescapable today, and this exposé demonstrates that you can’t believe everything you read. “Remember that metrics aren’t a measure of authenticity,” Kankaala explains.

“Not everything written on the internet is fact – no matter how authentic a profile may seem. Consider this: are multiple sources reporting the information you’ve read, or is it just this one profile? And do you believe something to be true because you want to believe it’s true? This can apply to profiles advertising discounted designer clothing as much as it does to topical news stories.”

Trending Sc@m

Old scam, new packaging

As our daily lives become more and more digitalized, online scams have rapidly emerged as a significant issue. They started with emails and SMS and swiftly moved with the times onto social media. Every day we read about a new trick, but the end goal is always the same: exploiting victims for monetary gain.

TOPICAL ISSUES SHAPING SCAMS

Often, the time-tested methods proven to yield results are safer for criminals than trying something new. So, online scammers have taken to repackaging old scams playing on human emotion to suit current trends. The curiosity that comes from a failed delivery message. Emails impersonating charities seeking donations for those affected by war. There's even a wedding invite scam that tricks you into downloading an infostealer APK sent via WhatsApp.

UPDATE YOUR SYSTEMS NOW

The day is not far when scams will use old Common Vulnerabilities and Exposures (CVEs) under the pretext of new lures. The best way to protect yourself is to get into the habit of regularly updating your apps, software, and devices – sooner rather than later.

Breach that matters

2FA leak exposes social media users

WHAT HAPPENED:

An SMS routing company used by Facebook, Google and TikTok to send one-time security codes faced backlash recently when it was discovered that one its databases was left exposed to the internet without password protection, letting anyone who knew the public IP address access its sensitive data.

WHY IT MATTERS:

Technology and internet company, YX International, sends around 5 million SMS messages each day. The exposed database contained the contents of password reset and one-time passcode (OTP) text messages sent to users of some of the world's largest tech companies, dating back to July 2023. While these messages typically expire after a few minutes, this situation demonstrates how vulnerable SMS is for two-factor authentication (2FA) – from the risk of interception to SIM swapping and leaked data.

WHAT SHOULD YOU DO:

Two-factor codes sent via SMS aren't as secure as stronger forms of 2FA. Instead, go to your account settings and, where possible, select an alternate 2FA method such as using an authenticator app.

Instantly check if your data has been exposed with our free F-Secure Identity Theft Checker!

ChatGPT: is your data safe?

Three vulnerabilities were recently found in ChatGPT and its plugins.

ChatGPT has taken the world by storm, generating 1.7 billion monthly users in just one year. To put this impressive rate of growth into perspective, it took almost 20 years for the internet to reach 1 billion monthly users. AI is now a part of everyday life – but it inevitably comes with security flaws.

"Security vulnerabilities have been discovered within ChatGPT and its plugins, allowing criminals to steal user data," explains Khalid Alnajjar, Threat Data Researcher at F-Secure. "Plugins are exclusive to ChatGPT Plus subscribers – however by using them, you give the AI chatbot permission to send sensitive data to third-party websites and, in some cases, access to external accounts such as Google Drive."

Vulnerability 1: ChatGPT

When a user installs a plugin that requires OAuth approval, ChatGPT redirects them to the plugin website to receive a code. Attackers could manipulate this to send users links for malicious plugins instead, with the attacker's credentials installed on their accounts, and then access any user data input into ChatGPT.

Vulnerability 2: PluginLab

When installing plugins from PluginLab – a tool that deploys ChatGPT plugins – a code is generated for ChatGPT to connect the user accounts. However, PluginLab failed to authenticate the request, so attackers could insert another account ID to access the plugin and any linked resources (e.g. private GitHub repos).

Vulnerability 3: Several plugins

Many plugins request broad permissions to access various accounts. During the OAuth verification process, attackers could intercept and modify the redirect URL to a malicious link, which they would then send to users. Upon clicking the link and logging into the plugin, the attacker could steal their credentials for the plugin and would then be able to take over it.

A surge in AI weaponization

"While these issues have now been resolved, it's possible that there will be further vulnerabilities discovered in the future. The best way to protect yourself is by only installing plugins from trusted sources and being extra cautious when sending sensitive information and linking other accounts to ChatGPT," Alnajjar concludes.

Khalid Alnajjar
Senior Threat Data Researcher
Helsinki, Finland

expert tip

Exercise caution when using ChatGPT and installing plugins and carefully review any permissions granted.

> **"By using plugins, you give permission to send sensitive data to third-party websites."**

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