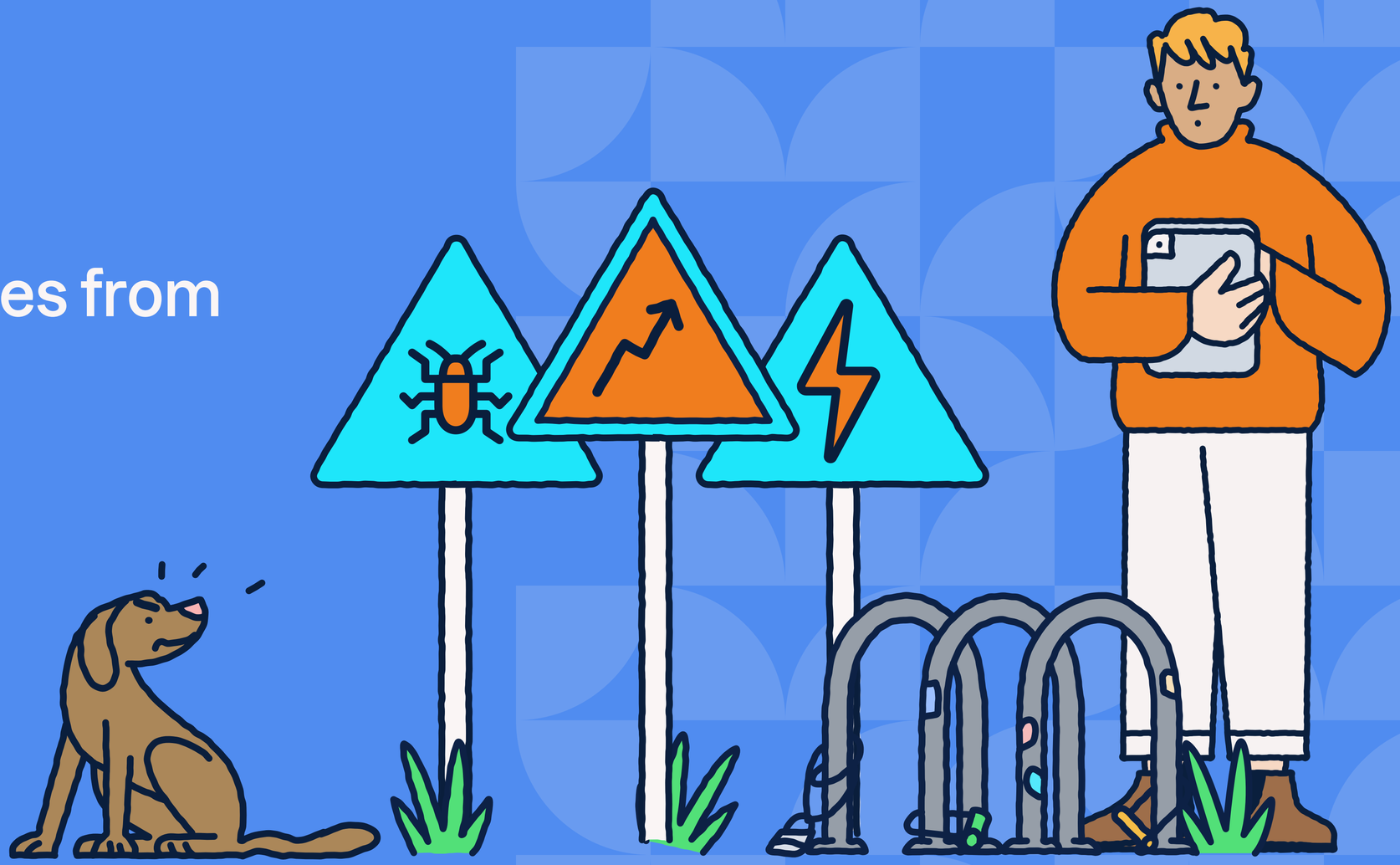
F-Alert

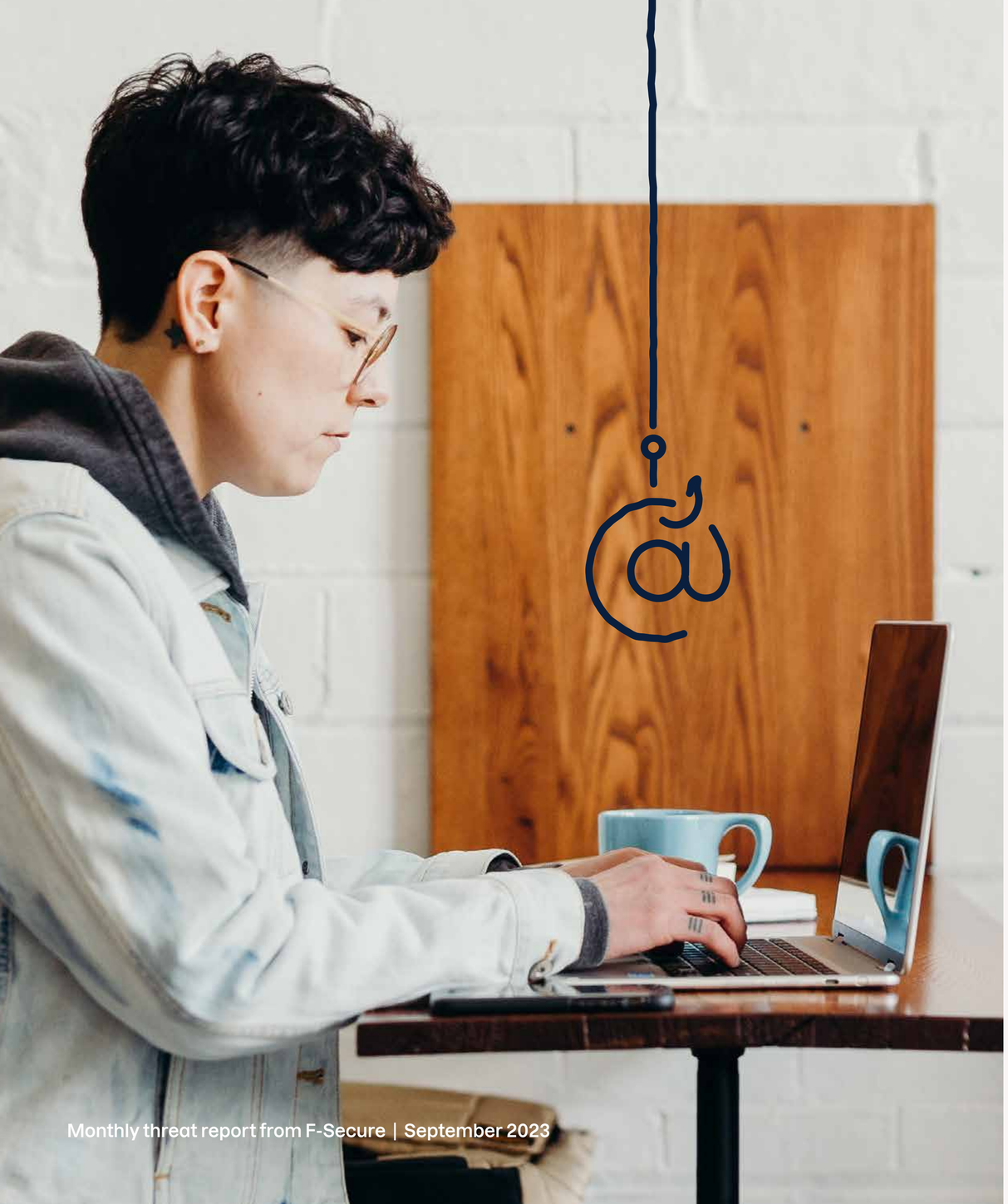
Monthly threat updates from

F-Secure

September 2023



F-Secure



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

See which cyber threats you're most likely to face. Find out why the Dark Web is so confusing to consumers, and profitable for criminals. Discover how you might know if you're being spied on through your mobile. And learn why LinkedIn has become a favorite destination for cyber criminals. All this and more in this month's F-Alert.

Timo Salmi
Senior Product Marketing Manager
Helsinki, Finland

expert tip

Apply the same scrutiny you give to any suspicious email to all SMS messages, DMs, or phone calls you receive. Any tactic that works in your inbox will eventually show up everywhere.

“This has opened the floodgates for scams related to fake prizes, fake online stores, and too-good-to-be-true offers.”

5 most common cyber crimes

Criminals keep adapting to go after bigger and bigger monetary gains.

Scams and frauds that target users on their phones for financial gain top the list of the most common cyber crimes, a new F-Secure survey has found.*

1. SMS scams

Just about anyone who owns a smartphone has come across a text message that could be classified as smishing, or a phishing attack that comes through SMS.

“That has opened the floodgates for scams related to fake prizes, fake online stores, and all sorts of too-good-to-be-true offers that may lead to cyber crimes,” said Timo Salmi, F-Secure Senior Product Marketing Manager.

2. Call fraud

“One of cyber criminals' favorite tricks in the last few years has been attacks that insist on a victim calling a certain number, often for tech support,” Salmi said. “This quickly leads to the attacker either extorting the victim, often to purchase a ‘warranty,’ or further infecting the victim.”

3. Malware and viruses

“Infostealers tend to be the malware that will end up on your machine,” Salmi said. “Once installed on a computer, it can collect any data that is entered into a web form, including login credentials, social security numbers, contact information and more.”

4. Credit card fraud

“Consumers are generally protected from fraudulent purchases on their breached accounts,” Salmi said. “But the crooks still get to go on a shopping spree until they’re detected and there may be long-term damage to victims, especially from fraudlent accounts opened up in their name.”

5. Unauthorized access to email accounts

“Hacked email accounts are valuable for a variety of reasons,” Salmi said. “In addition to the contents of the account, the ‘Forgot password?’ link on any app or website will give criminals access to almost any service connected to that email.”

*Source: F-Secure Consumer Survey June 2023, 11 countries (Brazil, Finland, France, Germany, Italy, Japan, The Netherlands, Norway, Sweden, UK and USA), n=4400

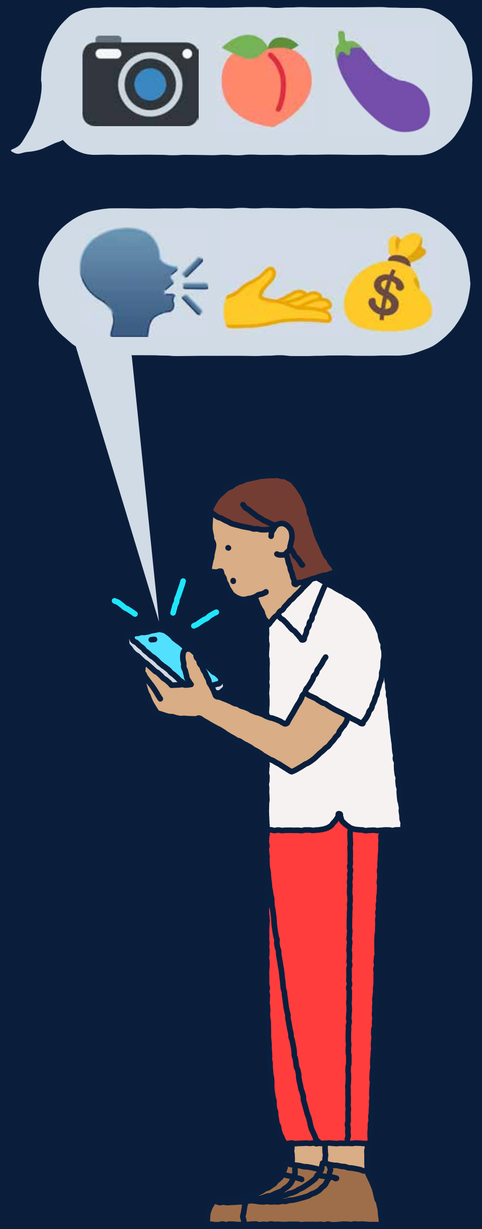
Trending Scam

‘Bad behavior online’ sextortion scam

WHAT:
F-Secure has seen a significant rise in scams that attempt to extort users for alleged “bad behavior online” delivered via email spam. These attacks often have subject lines that focus on the exposure of humiliating images and videos to friends, family, and colleagues, including “Your personal data has been leaked due to suspected harmful activities.”

HOW:
The scammers provide clear steps on how to pay using Bitcoin. To escalate the pressure, victims are told to act within a short period of time, often 2 days. Sadly, there is evidence of several victims giving into crooks’ demands.

PREPARE:
No one deserves to be a victim, but there are steps you can take to try to keep yourself off scammers’ radar. Avoid visiting shady websites for free software installers and software cracks. Also, use an identity protection solution that can reliably inform you about possible leaks or breaches related to your personal data.



Breach that matters

MGM Resorts International

WHY IT MATTERS:
With over two dozen resorts and an online sports betting operation, MGM Resorts International is one of the largest gaming companies in the world. The official @MGMResortsIntl X account announced on the 1st of September that the organization had “identified a cybersecurity issue affecting some of the Company’s systems.” According to developing reports, attackers behind the breach also hit Caesars casinos and three other firms with ransomware.

BREACHED DATA:
That remains unclear. The official company FAQ answers the question “Was my data breached?” with “Our investigation is ongoing… At this time, we do not have additional information available to share.”

WHAT SHOULD YOU DO:
Anyone who has stayed at MGM resorts would be wise to assume their information may have been compromised. Consider placing a hold on your credit report to prevent new accounts from being opened. And monitor your financial accounts even more closely than you do normally.

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

Why Stalkerware matters

Preventing spying on all of your digital activity requires getting to know how apps that enable stalking work.

Stores run by Apple and Google generally ban the sale of apps that enable secret monitoring that may occur as part of intimate partner harassment and abuse. But stalkerware is still available across the internet.

That means awareness is the best defense against software designed to track users without their consent or knowledge.

Few can do more harm

“No one knows more about us than our smartphones,” Laura Kankaala, F-Secure Threat Intelligence Lead. “And few people can do more harm with that knowledge than a former or current intimate partner who has become abusive.”

The Coalition Against Stalkerware, which F-Secure joined in 2019, defines stalkerware as “tools – software programs, apps and devices – that enable someone to secretly spy on another person’s private life via their mobile device.”

Kankaala noted that Stalkerware can be installed by pretty much anyone who knows how to use a smartphone.

“All someone needs is access to your device, and a few minutes.”

Look out for warning signs

Stalkerware apps are designed to run without the device owner’s knowledge. However, there are some signs that you can look out for to detect Stalkerware installation, starting with overall poorer performance of your device.

“Your phone, especially for Android devices, may become very warm due to constant location tracking,” Kankaala said. “For iPhone, it's best to go through the list of active sessions on iCloud to see if any unrecognized devices have access to information on your phone."

She noted that running a scan with antivirus software generally detects malicious apps installed on the phone.

“But if you have been infected, that likely means you face some-to-significant danger from a current or former partner,” she said. “While we may be trained by the media to fear strangers, we’re more likely to face violence from the people we’ve known best, both online and off.”

She recommends anyone with any reason to believe a device has been infected with stalkerware to visit the Coalition Against Stalkerware site to come up with a safety plan before removing the app.

Laura Kankaala
Threat Intelligence Lead
Helsinki, Finland

expert tip

We can’t be with our device at all times, so be sure to have a passcode on your mobile device and strong, unique passwords for your important online accounts, including iCloud. And don’t share them with anyone.

“All someone needs is access to your device, and a few minutes.”

Exposing the DARK WEB

The internet's darkest corner

A new survey finds that 68% of adults are confused about the dark web. Here's what you need to know.

Has your private data been leaked in the last 12 months?

1 in 6 report that their data has leaked online.

That's what a new Censuswide survey of 5,000 adults commissioned by F-Secure found.

Nearly 4 in 10 said they don't know if their data has leaked.

That means they could be exposed and likely aren't taking any of the steps necessary to protect their accounts or identities.

80% of those surveyed said they knew what the dark web is.

But less than 1 in 3 could accurately define it as a part of the Internet that can only be accessed using special, anonymized browsers.

Why does that matter?

The dark web is also a destination where cyber criminals can buy stolen and leaked data.

Every month, millions of private credentials go up for sale there.

An endless cycle

Once data is on the dark web, it's just about impossible to get it off. Which is why it's essential to find out if you've been exposed.

Yet **more than 3 in 4** of adults (77%) surveyed rarely, or never, check if their data has been stolen or leaked.

This leaves many victims trapped in a virtually endless cycle of their information being sold.

But there is hope for anyone who takes the right steps.

*Source: Censuswide 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

Tom Gaffney
Principal Security Consultant
London, England

expert tip

Regularly check to see if your data has been compromised using free online tools such as F-Secure's Identity Theft Checker.

"It takes less than five minutes to check if you've been compromised and it doesn't cost anything to do so."

Ash Shatrieh
Threat Intelligence Researcher
Helsinki, Finland

expert tip

To prevent account hijacking, be sure you have activated two-factor authentication for your LinkedIn account, ideally through an authenticator app on a secured device. Do it now.

“Users should expect to face skilled attackers on LinkedIn and take precautions immediately.”

Cyber criminals love LinkedIn

The social network has become essential both for professionals looking for career advancement, and attackers looking to exploit those ambitions.

LinkedIn users have experienced a steady increase in malicious activities in the last decade, ranging from suspicious connection attempts to phishing scams to fake job offers. Now, reports suggest that cyber attacks on the platform have escalated dramatically.

A treasure trove

Attackers have long known that LinkedIn offers a treasure trove of invaluable information, explained Ash Shatrieh, F-Secure Threat Intelligence Researcher.

“The platform contains an abundance of intelligence about an organization’s personnel that generally isn’t available on the company website,” he said. “This information has helped criminals sharpen attacks that involve psychological manipulation, including phishing and Business Email Compromise.”

But new research suggests that attacks on LinkedIn accounts spiked in the summer of 2023, as criminals have embraced a new tactic that raises the stakes for anyone who relies on the site for career advancement or professional networking.

“One report found that some users have seen their accounts held for ransom,” he added. “These victims were threatened with account deletion if they didn’t pay.”

Attackers are extremely motivated

Linkedin, perhaps more than any other social media platform, blends the personal with the professional.

“Criminal gangs in Southeast Asia have used initial contacts on LinkedIn to help launch advanced attacks targeting Meta Business accounts,” Shatrieh said. “Attackers love LinkedIn because of its business authenticity.”

He noted that identity theft on LinkedIn can be extremely valuable for criminals, because 1) the possible disclosure of sensitive business information, and 2) attackers can use an account to carry on legitimate-looking attacks, such as messaging a colleague a phishing link.

“That’s why users should expect to face skilled attackers on the platform and take precautions immediately, if they haven’t already,” he concluded.

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