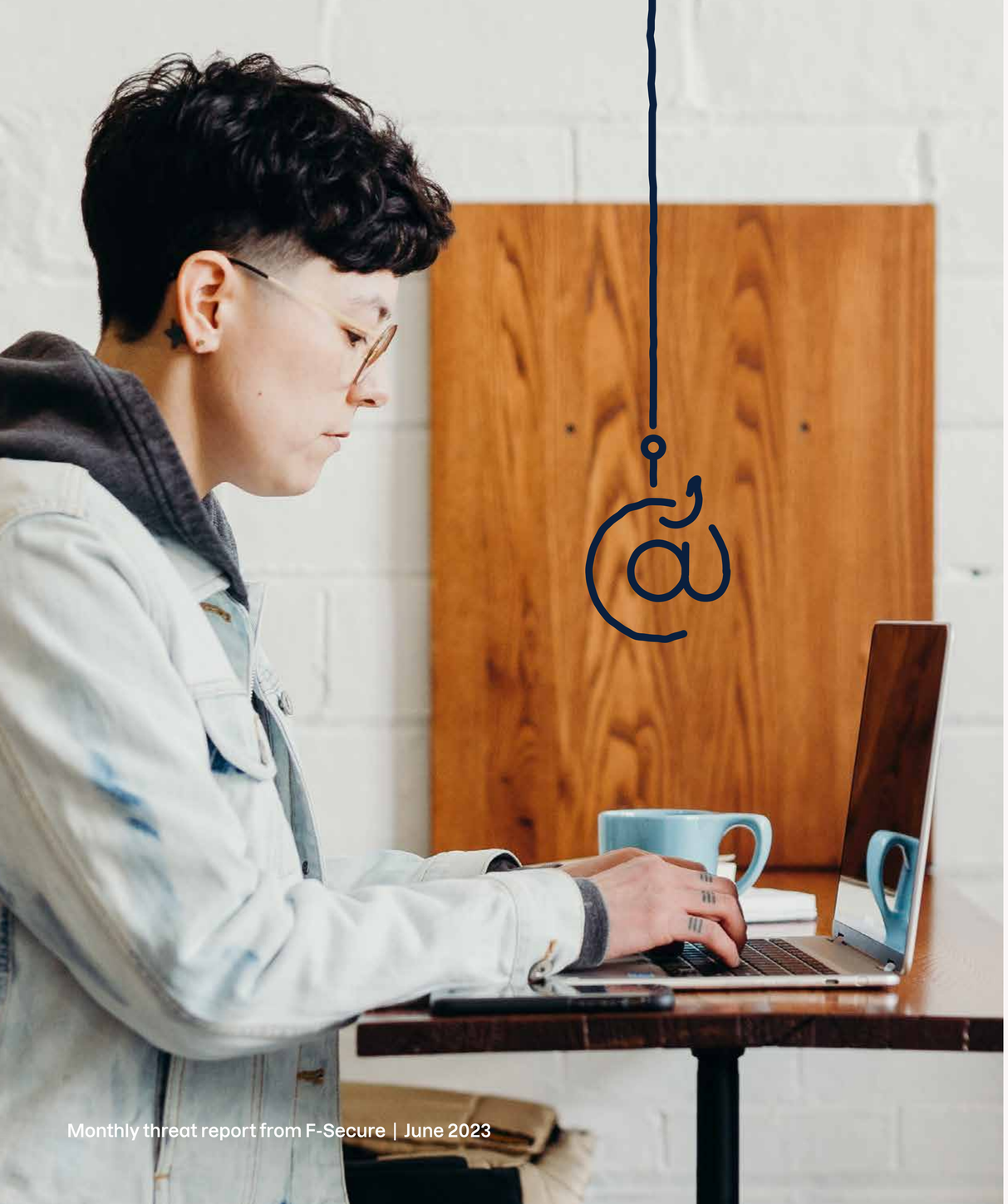
F-Alert

Monthly threat updates from

F-Secure

June 2023

F-Secure



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

Find out how to secure all your digital moments on vacation. Learn what employees should do when the companies they work for are breached. Discover how to talk about AI in terms everyone gets. Meet the latest nasty Android malware scam. And get the lowdown on why you can’t take Apple security for granted. All in the summer edition of F-Alert.

Felix Blank
Senior Solution Consultant
Munich, Germany

expert tip

If it's available where you are, consider placing a fraud alert or security freeze on your credit file. This stops criminals from opening new accounts in your name. And consider a trusted identity protection solution, like the one included in F-Secure Total, to keep track of how your stolen data may be used against you.

"Giving into the ransom demand not only encourages the criminal, but it also probably won't work."

Breaches expose employees

Criminals pounce on a vulnerability in HR software to steal personal data. Here's what victims can do.

The ransomware gang Clop has claimed credit for a series of attacks that exploited a previously undetected vulnerability in MOVEit Transfer. Numerous software solutions, including the human resources platform Zellis, incorporate this tool.

Employees of the BBC, banks, universities, and the government of Nova Scotia along with thousands of other firms have had a variety of private data exposed, including—in a few cases—banking information.

Clop gets personal

Progress software, the makers of MOVEit Transfer, announced that it had begun patching MOVEit vulnerabilities in May of 2023. But Clop seems to have been exploiting security holes in software since 2021

"The gang took the unusual step of not contacting the companies directly to demand a ransom," said Felix Blank, a Senior Solution Consultant at F-Secure. "Instead, they published a blackmail message on their own site insisting victims contact them directly by a deadline in mid-June that had already passed."

That message told victims that the gang had taken "alot [sic] of your data." Blank noted that the criminals are following a new trend in ransomware, where groups attempt multiple ways of monetizing data, including the threat of publicly exposing data.

Take action, not the bait

Unfortunately, Blank pointed out that there's no guaranteed relief for the victims here, even if they pay the ransom.

"Giving into the ransom demand not only encourages the criminal, but it also probably won't work," he said. "The data stolen here is likely to end up on the dark web eventually, in one way or another."

This grim reality can motivate victims to take the steps necessary to protect their accounts and their identities.

"Follow your employer's guidance if you receive any," Blank said. "In addition, monitor your online identity while being especially cautious about clicking on any links from unsolicited texts or emails you may receive."

Android trojans make users pay

Malicious apps promise cool tools but stick Google Play customers with unwanted subscriptions.

Online criminals are moving into the lucrative world of subscription services—using fraud, of course.

The Android trojan Fleckpe keeps popping up in the Google Play store hidden inside appealing apps, including beauty tools, photo editing software, and wallpaper packs. Once installed, the malware sneakily subscribes victims to paid services.

Abusing users' trust

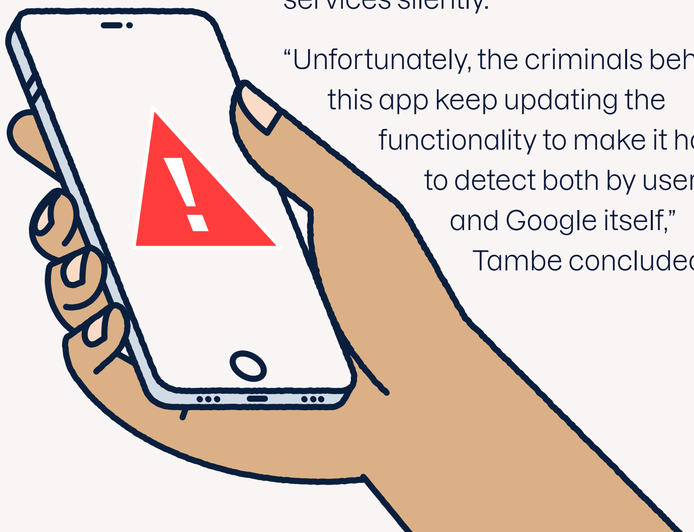
While Google seems to be successful at weeding out apps embedded with Fleckpe as they pop up, the trojan has reportedly infected more than half a million users since 2022.

"Threat actors keep finding innovative ways to gain the trust of victims to get them to install malware," said Amit Tambe, a researcher at F-Secure. "These attackers are taking advantage of the strong trust many users have in the Google Play store."

The process of infection greatly resembles installation of a legitimate app, so users aren't likely to be suspicious, or even aware of, the malicious activities Fleckpe is carrying out in the background.

Business, as usual

Tambe noted that as the app is installed, it requests permission to access SMS messages and notifications.



"As Fleckpe hides inside genuine looking apps, the requests for granting SMS and notification permissions may not seem out of the ordinary," he said. "This access gives criminals the ability to initiate the reoccurring credit card charges that make this scam so profitable."

Using the access requested by the app as the user installed it, the malware is able to carry out any confirmations needed for the services silently.

"Unfortunately, the criminals behind this app keep updating the functionality to make it harder to detect both by users and Google itself," Tambe concluded.

Amit Tambe
Researcher
Helsinki, Finland

expert tip

The best way to avoid malicious mobile apps is to stick to official stores. But even the apps inside Google Play can be harmful. Don't just check the rating of an app; check the reviews. If you're still worried, trust your senses and check the developer ratings, too.

"These attackers are taking advantage of the strong trust many users have in the Google Play store."

Securing your digital moments on vacation

Your digital devices help make the most of your holidays, so here's how to make sure they stay secure.

Before you leave

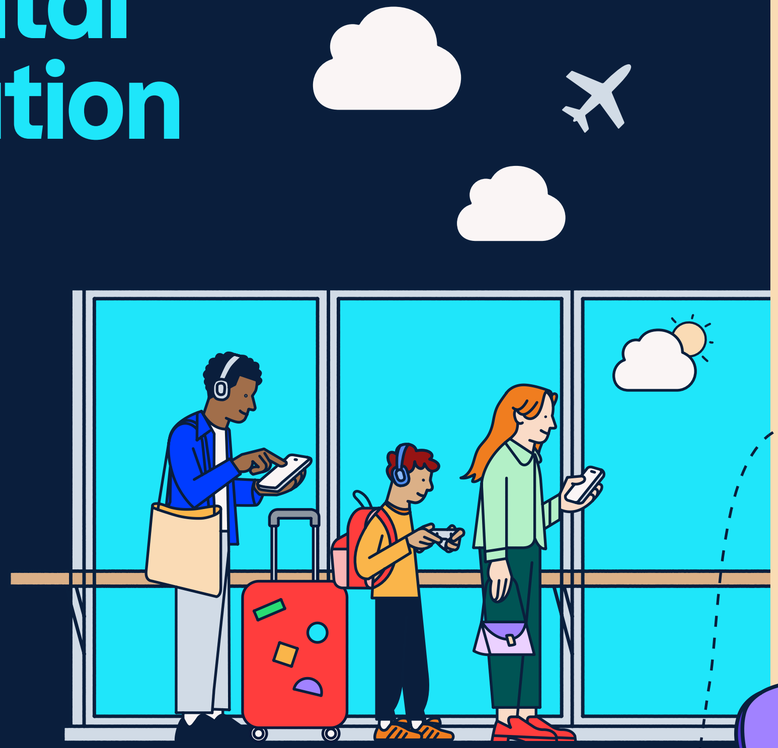
1

Smart home

Time your smart lights to make it look as if you're home. And don't leave without giving your Wi-Fi and all your smart devices a strong, unique password.

Devices

Take backups of your devices. Also make sure you have synced your passwords from your password manager across multiple devices, so you won't lose access to your services.

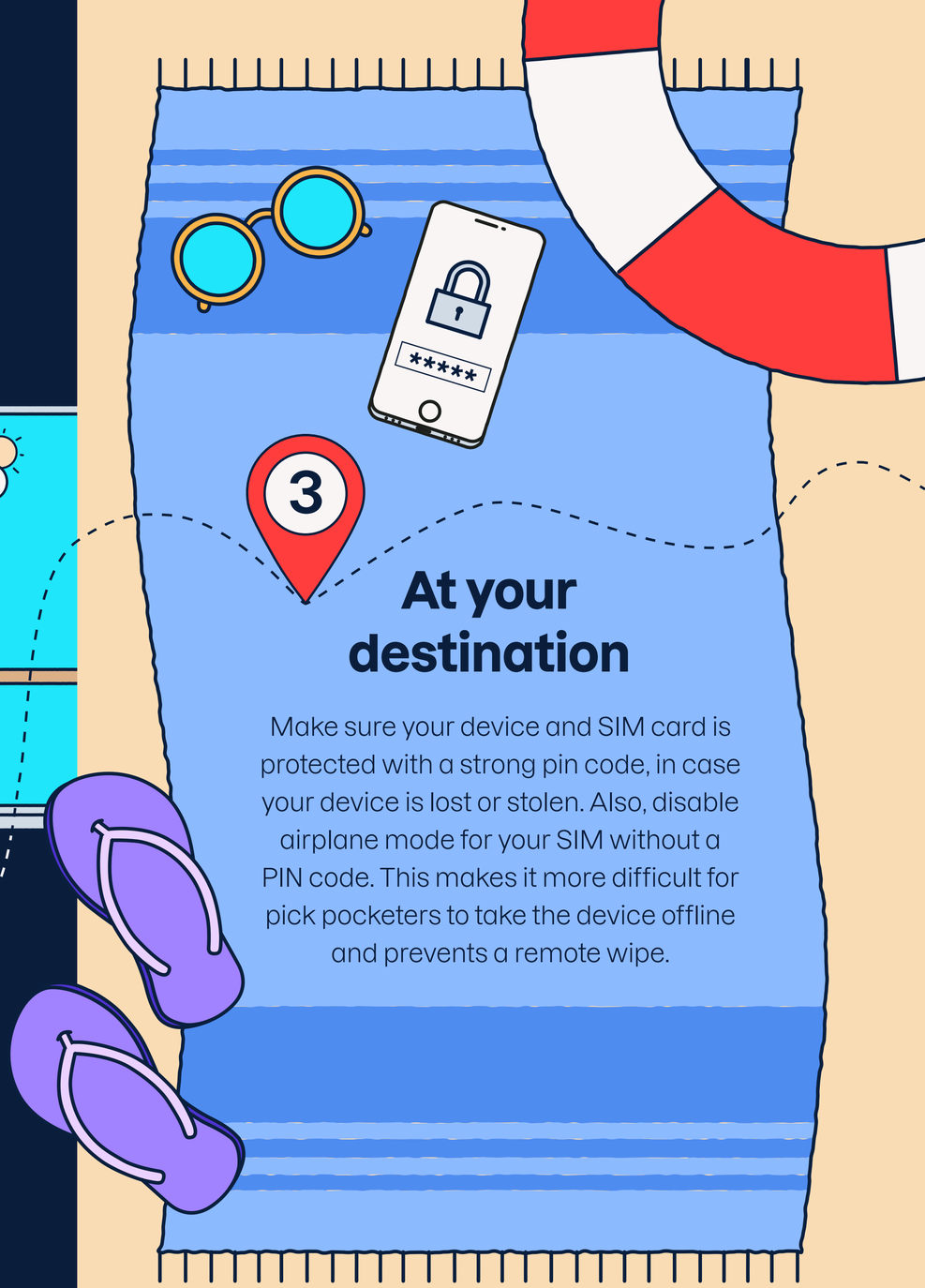


2

On the road

Airports and public transport

Need free public WiFi? Use VPN when connecting to any network while traveling.



3

At your destination

Make sure your device and SIM card is protected with a strong pin code, in case your device is lost or stolen. Also, disable airplane mode for your SIM without a PIN code. This makes it more difficult for pick pocketers to take the device offline and prevents a remote wipe.

4

Worst case scenario

A lost phone

If you lose your device or believe it has been stolen, **quick action is essential:**

Get on another device and attempt to **track your phone** using Find My Device for Android or iCloud.com/find for iOS devices.

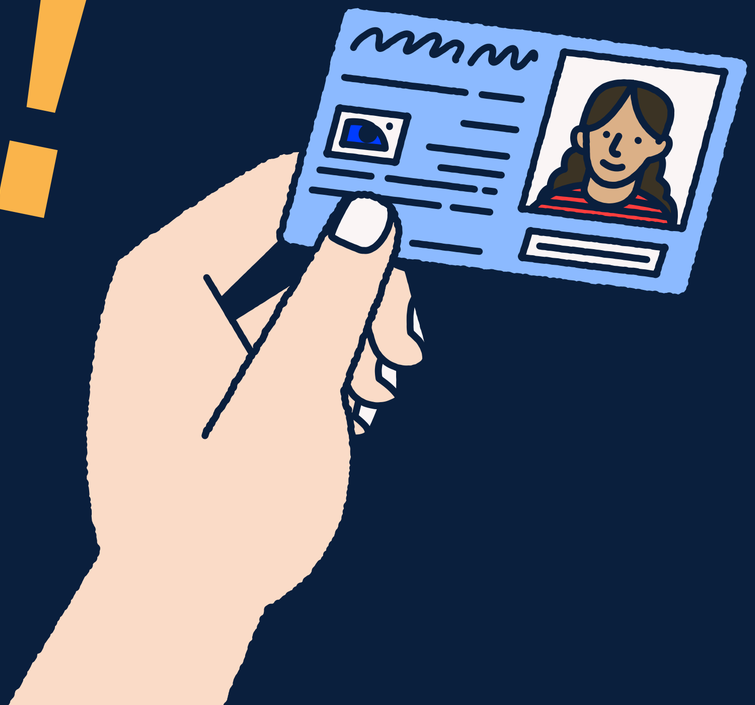
Lock your phone using Android's Secure Device function or iOS's Lost Mode.

Report the loss to any relevant authorities and contact your mobile carrier to makes sure the device is unusable to whoever has it.

5

When you get home

Be sure to closely check all the statements of any credit or bank cards you used – in person or online – while on vacation.



Travel with peace of mind.

F-Secure Total offers complete online security, privacy, and ID protection, wherever you go, with one app.

What you need to know about AI

Experts keep warning about the risks of artificial intelligence, but what should that mean to you?

AI tools capable of generating text and images, including ChatGPT and Midjourney, have been embraced by hundreds of millions of people. Yet some experts are raising the alarm about the rise of machines that seem to think.

Things get more intelligent than us

The so-called "Godfather of AI" quit Google in May so he could speak freely about the "existential risk of what happens when these things get more intelligent than us." And in June, Singapore identified six risks of generative AI—they are "hallucinations," privacy concerns, disinformation, copyright issues, inherent biases, and the challenge of building safety valves into these models.

That's why we asked Khalid Alnajjar, a Threat Data Researcher at F-Secure, to explain some basics everyone needs to know about AI.

What are large language models (LLMS)?

Language models aim to generate text by understanding the context and predicting the most likely response to it, one word at a time.

Think of the LLM as an experienced assistant who has read through all the data and can provide you with relevant advice instantly for the current case you are working on by analyzing it and comparing it to the cases it has read about in the background.

However, don't make the mistake of thinking everything an LLM tells you is true, as one lawyer in the United States did. He submitted a brief that included six cases that ChatGPT seemed to hallucinate from thin air. Unfortunately, the judge noticed.

What are the security risks of AI?

AI is a double-edged sword and, when it is in the hands of cyber attackers, undesired outcomes are bound to happen. These attacks can consist of injecting malicious content into the AI models themselves. This could include anything from malicious code to propaganda.

Generative AI can easily be used to automate phishing and scams, and to impersonate people by mimicking their unique style to produce misleading content such as deep fakes of politicians giving provocative speeches.

It is crucial to be aware of these attacks and not trust online content blindly—now, more than ever.

Khalid Alnajjar
Threat Data Researcher
Helsinki, Finland

expert tip

Generative AI can easily be used to automate phishing and scams, and to impersonate people by mimicking their unique style to produce misleading content such as deep fakes of politicians saying or doing provocative things. It is crucial to be aware of these attacks and not trust online content blindly—now, more than ever.

"Think of the LLM as an experienced assistant."

ADVANCE ALERT :
Infostealers and the MacOS goldmine

You can’t take Apple security for granted anymore

MacOS has long been seen as a fortress against cyber attacks. However, recent developments have shattered this notion, as infostealers have emerged as a rising threat to Apple's ecosystem—and its users.

A sneak attack on your most valuable data

Infostealers can steal sensitive information such as your keychain passwords or login details to your email, social media accounts, streaming services, and messaging applications.

This threat can end up on your Mac via phishing techniques that employ victim manipulation tactics. Fake cleaner or helper applications, as well as pirated or cracked software, also lead to infostealer infections.

Exploiting good intention

Apple has introduced numerous security features such as File Quarantine, Gatekeeper, Notarization, and XProtect, to safeguard users from phishing attacks and malicious apps. However, Apple’s security controls include the ability for the user to bypass the protection.

Unsurprisingly, malicious apps have started to employ social engineering techniques to create convincing scenarios that prompt users to open the malicious apps anyway. The AMOS infostealer (Atomic MacOS Stealer), for example, convinces users to right-click the malicious app. A window then tells the victim to ignore the error message from the security controls, effectively evading Apple’s security measures.

Additionally, MacOS, like other Operating Systems, has a powerful admin user that can access all files and applications running on the machine. Infostealers often trick users into revealing their admin password by displaying a lookalike for a system password dialog. This allows the malware to gain access to hidden areas in the system and grab sensitive information. The stealer can even maintain itself in the system and maintain access, using what are known as persistence techniques.

The bigger picture

Malware targeting MacOS has almost doubled between 2020 and 2022. The number of unique, new malware families is still low at 13. But what's most significant is that malware groups have begun creating MacOS version of their attacks. This shows a shift towards MacOS that follows its market-share increase. ■

Ash Shatrieh
Threat Intelligence Researcher
Helsinki, Finland

expert tip

To protect yourself from infostealers, adopt proactive measures. Keeping everything up to date is crucial - so don't snooze updates for your operating system and applications, which should all come from the official Apple App Store. In addition, a trusted anti-malware software, such as F-Secure Total, can significantly enhance your protection.

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 180 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