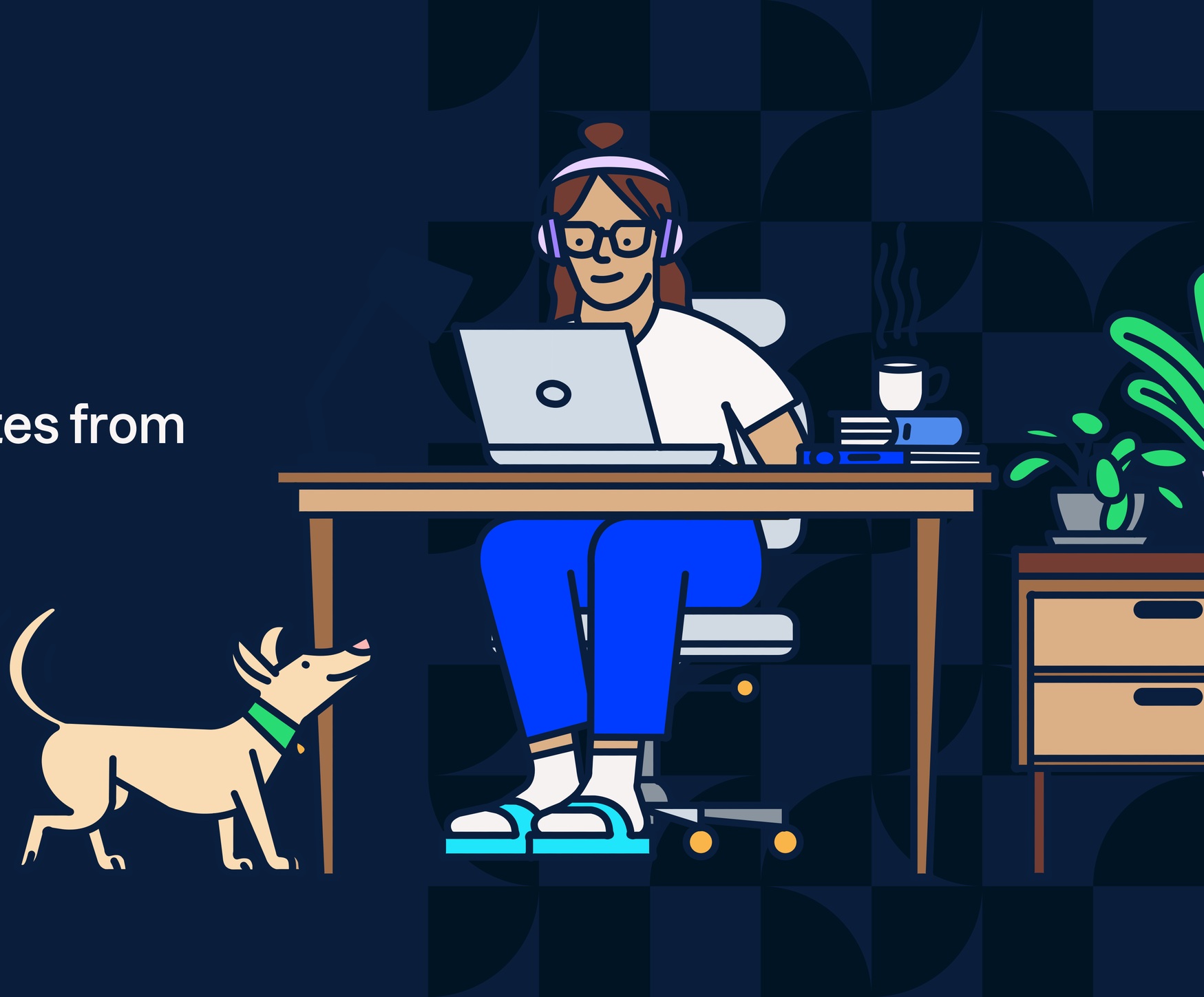
F-Alert

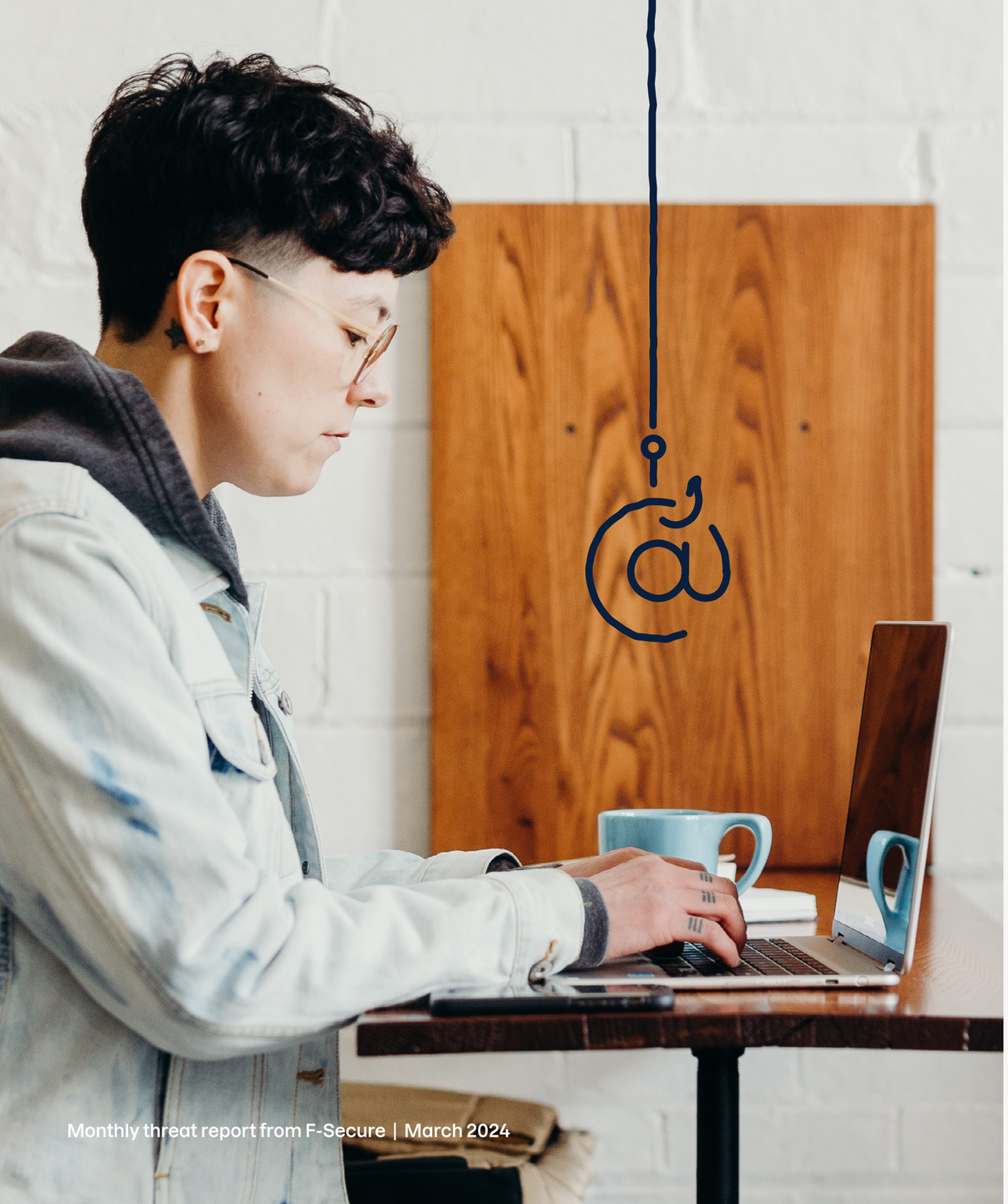
Monthly threat updates from

F-Secure

March 2024



F-Secure



From phishing in plain sight to the world's largest known data leak

Discover the latest security updates from our experts:

- Apple battens down the iPhone
- Texting in a scammer's paradise?
- AI scams just got personal
- Smart toothbrush – or gateway for hackers?
- The mother of all breaches has hit
- Google Ads are turning malicious

Apple battens down the iPhone

Flimsy security no more: Stolen Device Protection is a game changer.

If you haven't ever lost your smartphone or had it stolen, it's likely you know someone who has.

iPhone theft is a lucrative business for criminals when devices are unlocked. Not only can they sell the handset for fast cash, but they can also access apps and empty the owner's bank accounts – all with a single passcode.

At least, that was before Apple introduced the iPhone's new Stolen Device Protection feature.

Locked out within minutes

"Prior to Apple's most recent iPhone security update, criminals could easily lock out the original owner of an iPhone and block the Find My app in minutes – just by knowing their passcode," explains Ash Shatrieh, Threat Intelligence Researcher at F-Secure.

"The passcode acted as a backup to facial or fingerprint authentication, so learning this would override any biometric security. Criminals could reset the iCloud password, or even access Apple Keychain and find passwords to banking apps."

A new era of iPhone security

To solve this issue, Apple has introduced Stolen Device Protection – a new layer of security that protects your personal information if your iPhone is stolen.

"When enabled, it provides additional security requirements for selected actions when you're away from familiar locations such as home, work, or other places where you spend a significant amount of time," Shatrieh explains.

"Some actions such as accessing credit cards and stored passwords now only require biometric authentication, with no passcode to fall back on. Other actions like changing your Apple ID password require you to wait an hour and then submit a second Face ID or Touch ID."

Is the future foolproof?

iPhone users now have a larger window of time to mark their device as lost and secure their Apple ID account to prevent thieves from performing harmful operations. And in the event your iPhone is stolen, someone who knows your passcode won't be able to make significant changes.

However, it's important to note that your iPhone may end the security delay early if it detects that you've arrived at a familiar location. In theory, a thief opening the Maps app and visiting a victim's home address could unlock the protection feature if the device isn't already in Stolen Device Mode.

Ash Shatrieh
Threat Intelligence Researcher
Helsinki, Finland

expert tip

Stolen Device Protection isn't automatically enabled on your iPhone, so you won't reap the benefits in the event of a lost or stolen device until you go into the settings, turn on the feature, and set up two-factor authentication for your Apple ID.

"Actions such as accessing credit cards now only require biometric authentication."

Laura Kankaala
Threat Intelligence Lead
Helsinki, Finland

expert tip

Use F-Secure Browsing Protection to stop phishing attacks by blocking malicious sites. It's always good to stay up to date with common phishing scams and avoid clicking on links you receive via unsolicited emails, text messages, or direct messages.

“Criminals can buy every element of a phishing campaign easily and inexpensively.”

Texting in a scammer’s paradise?

Dark markets are no longer restricted to the dark web – Telegram's public channels are now rife with phishing resources.

Once upon a time, phishing was an underground operation. Criminals would receive secret invites to exclusive forums on the dark web, where they’d source information and resources for phishing scams.

But today’s scammer is bolder. Now, phishing kits, criminal insights, and even freelance hackers are publicly available via instant messaging app, Telegram.

Unparalleled privacy

What sets Telegram apart from other instant messaging apps is its increased level of privacy. In fact, you only need a valid phone number to register – which can be hidden and replaced with a username.

“Not only does Telegram offer anonymity, but users have end-to-end encrypted chats and can send timed self-destruct messages. With ease of communication and the opportunity to reach a wide audience, it’s no wonder that there’s such an active criminal user base,” says Laura Kankaala, Threat Intelligence Lead at F-Secure.

Phishing by numbers

According to a recent investigation, a successful phishing campaign can be put together – even by novices – for as little as $230 using Telegram’s public channels.

“Criminals can buy every element of a phishing campaign easily and inexpensively on Telegram – from pre-built phishing websites masquerading as banks, to offshore hosting providers and even stolen contact data,” explains Kankaala.

“Small-time scammers will either try to benefit from stolen data themselves or, for instance, sell any phished banking credentials to organized criminal groups.”

Website owners, take heed

The basis of a phishing campaign is to mimic a legitimate website. Where the website and its backend infrastructure for collecting the information are hosted depends on the capabilities of the threat actors.

“We’ve witnessed phishing sites hosted using regular hosting providers, on cloud services and platforms, or even by hacking into sites operated by legitimate companies,” says Kankaala.

“Websites with unpatched security vulnerabilities or content management systems such as WordPress are often targeted to host illegal activities. Therefore, it's vital for website owners to routinely patch and update their websites.”

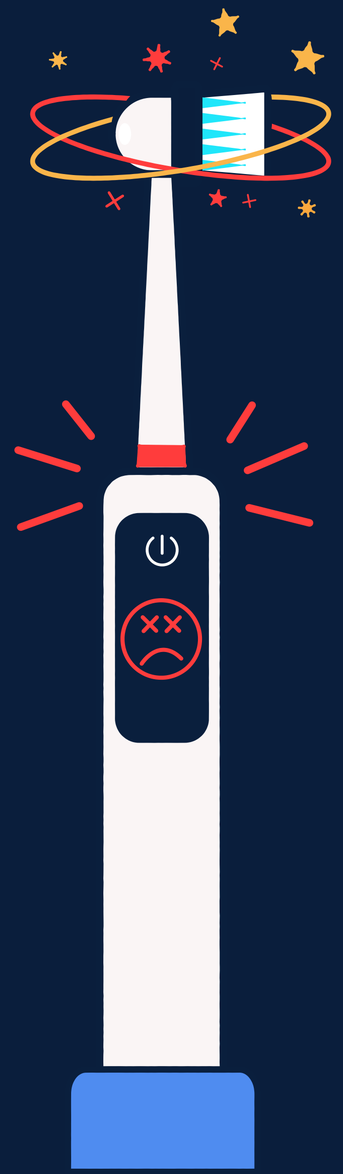
Trending Scam

AI scams just got personal

WHAT:
Voice cloning is the latest AI scam designed to deceive and convince people to part with their money using the voice of someone they know. A Swedish woman was almost scammed out of SEK 15,000 after receiving a phone call and hearing her daughter's voice encouraging her to send money.

HOW:
Ann-Lis, residing in Malmö, Sweden, received a text message saying her daughter had changed phone number, followed by a request for SEK 15,000 for a new phone and computer. She was suspicious until she received a phone call and heard her daughter's voice, at which point she let down her barriers.

TO PROTECT YOURSELF:
AI scammers can replicate voices using short clips found online. So, if you haven't been cautious about what you publish on social media, now's the time to start. If you receive a strange request from someone you know, contact that person using the contact details you already have for them. You could even agree a secret phrase with relatives to verify their identity in a potential situation such as this.



Breach that matters

Smart toothbrush – or gateway for hackers?

WHAT HAPPENED:
In February, a story was published that instilled fear in smart toothbrush users: your trusty plaque buster has been compromised. The article said that a cyber attack was linked to breached internet-connected toothbrushes – however it has since been debunked, with the media outlet claiming it was hypothetical. How did the mix up happen? Mistranslations of the article by other publications resulted in a story simply lost in translation.

WHY IT MATTERS:
The moral of this story is to not believe everything you read in the media – the mass media will repeat any news story written by media outlets without fact checking with cyber security experts first. While an attack of that scale is unlikely, it does highlight the very real possibility that a connected device as seemingly harmless as a smart toothbrush could be the weak link into your home for criminals looking to hack through unpatched vulnerabilities.

WHAT SHOULD YOU DO:
Buy smart devices that prioritize security. Change default login passwords to strong and unique passwords, and always keep smart devices updated to the latest version.

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

The mother of all breaches has hit

Billions of records exposed in the largest known, supermassive data leak.

Joel Latto
Threat Advisor
Helsinki, Finland

expert tip

By using an online identity monitoring service such as F-Secure ID Protection, you'll get alerted if your personal data has been part of this or any other breach.

"It's possible that phishing and account takeover attempts will momentarily increase."

The largest data leak of all time by a considerable margin. That's what happened when a firewall misconfiguration enabled unauthorized access to data breach search engine, Leak Lookup's, data last December.

The irony is not lost on us. Or as Joel Latto, Threat Advisor at F-Secure, put it: "Someone essentially stole their main business asset and posted it online."

An unparalleled scale

It wasn't until January of this year that the story broke, and it was revealed that 26 billion records – an astonishing 12 terabytes of information made up of data from previous breaches – were leaked.

To put the scale of this leak in perspective, the previous largest leak was 2.2 billion records.

All the data you could dream of

"Known as the 'mother of all breaches', this supermassive leak is a curated collection of data leaks and breaches from several years, covering a vast number of big and smaller brands around the world," explains Latto.

The data includes email addresses, passwords, full names, and a wealth of other personally identifiable information. "Cyber criminals can use this data of course how they normally would, such as for credential stuffing," continues Latto.

"But due to the size of the dataset, criminals can also engage in convincing spear phishing attacks by combining a target profile from many different breaches, cross referencing with an email address or phone number, and then pulling all those results together."

Take care of your cyber hygiene

As this is not a new data breach but a compilation of old leaks, there's no immediate rush to change passwords – if you already use unique and strong ones everywhere.

"Two-factor authentication is a must and I recommend using an authenticator app. Avoid SMS authentication as it's susceptible to SIM swapping attacks," says Latto.

"It's possible that phishing and account takeover attempts will momentarily increase, so extra vigilance is encouraged."

Google Ads are turning malicious

Criminals are tricking Google into advertising downloads for malware.

Cyber criminals are continuing to infiltrate Google with malicious ads masquerading as downloads of popular free software.

Google Ads appear above organic search results – with up to four ads displaying first – resulting in links to real software being pushed further down the page. To lure searchers, threat actors set up campaigns that look like ads leading to genuine websites but click through to a download for their malware instead.

Bypassing Google's filters

"Criminals clone the websites of legitimate software applications and distribute malicious backdoor versions of the software through download buttons," explains Amit Tambe, Researcher at F-Secure.

"If Google detects a malicious website, the campaign is blocked, and the ads are removed. To get around this, criminals will trick people into clicking on an ad leading to a benign website and then redirect them to the cloned malicious site."

Rotating dodgy domains

Another tactic developed by criminals is to rotate domains in and out of hosting malware.

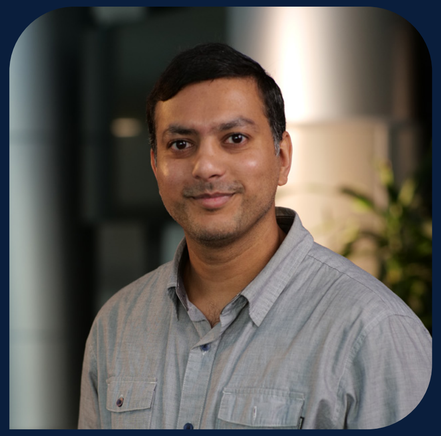
"Software websites that seem to be safe for a long time can one day turn bad – swapping genuine downloads for malware. This helps criminals stay under Google's radar," says Tambe.

According to a recent investigation, malicious websites may only be served to specific geographic locations at a time. Once a domain gains legitimacy in Google, threat actors will convert it to the malicious version for a day or two and then revert it to the benign version.

Avoiding dangerous sites

"Google Safe Browsing shows a warning to users if they attempt to access a known dangerous website. It's important to always heed this warning to avoid landing on a malicious site," explains Tambe.

"Threat actors have a multitude of tricks to conceal their identities and trick Google into keeping their ads up, so it's crucial that you remain vigilant. Be mindful of clicking sponsored ads and browse organic search results instead to identify genuine sources of software."



Amit Tambe
Researcher
Helsinki, Finland

expert tip

Threat actors are so advanced in their deceit that they can create ads that display legitimate URLs but redirect users to cloned sites. So, the best way to protect yourself is with a complete online protection solution like F-Secure Total.

"Software websites that seem to be safe for a long time can one day turn bad."

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