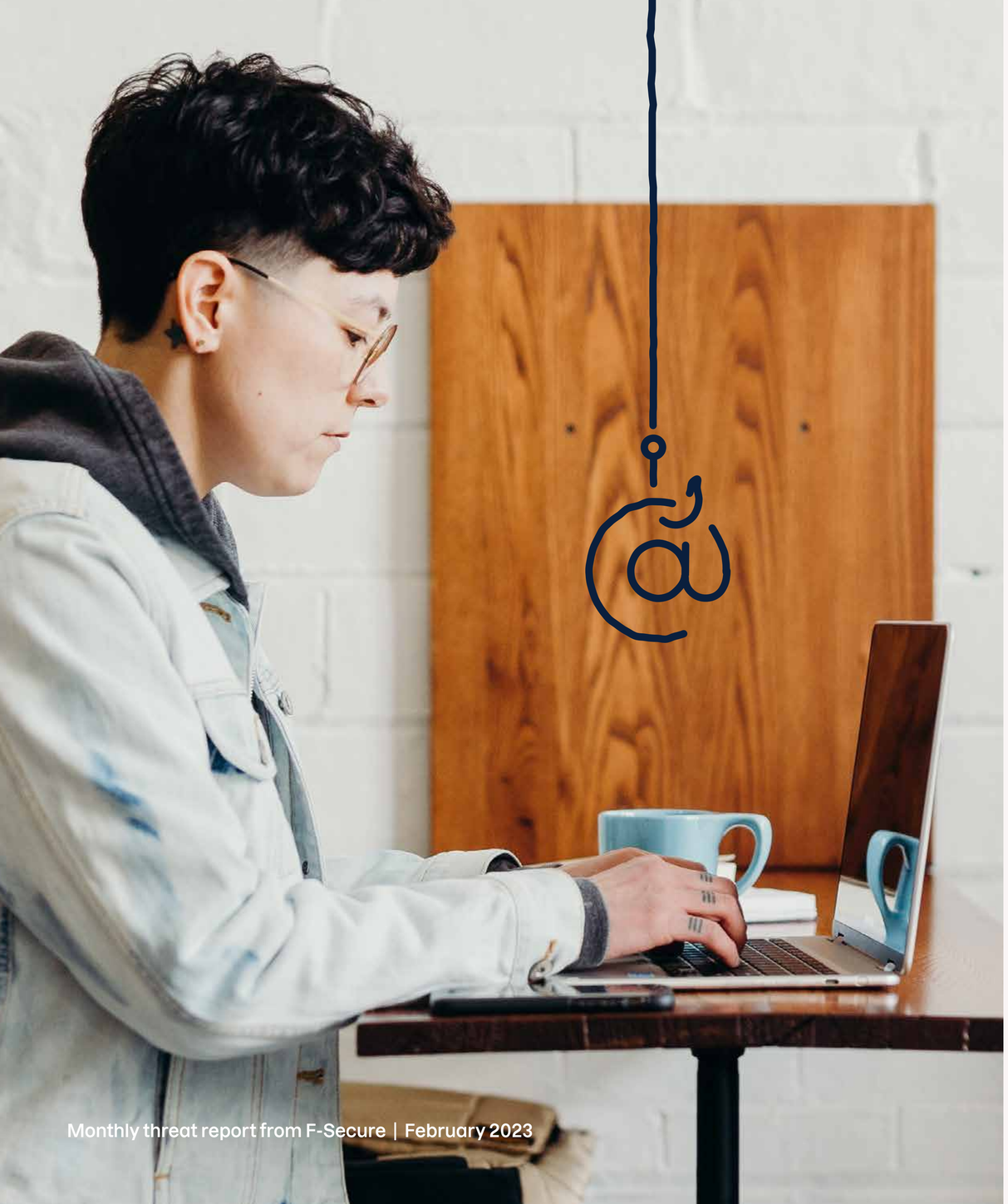
F-Alert

Monthly threat report from

F-Secure

February 2023

F-Secure



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

Find out how criminals have shifted to target Microsoft’s free note-taking application, OneNote. See how the popular social media hub Reddit handled a breach of its user data. Find out how online criminals celebrated Valentine’s Day. And learn how the month's biggest leaks might affect you and your data.

Amit Tambe
Researcher
Helsinki, Finland

expert tip

Look out for OneNote files, which include the suffix ".one". You should always check any attachment you receive before opening them by scanning and by checking with the person who sent it to you. But unless you have a good reason to do otherwise, refuse to open any OneNote files for the time being, unless you are certain the document is legitimate.

Attackers target OneNote

A smart defensive move by Microsoft has resulted in criminals targeting one of its less popular applications.

Phishing attacks that target files created in Microsoft's OneNote note-taking app have risen exponentially over the past few months, as criminals shifted to make up for the loss of one of their most reliable sources of income.

Microsoft tightened the noose

In July 2022, Microsoft changed the default behavior of Office applications to block macros, which are single commands that imitate multiple keystrokes or mouse actions, enabling you to complete laborious tasks—such as adding a letterhead—in a single click.

"Simply put, macros are—or were—attackers' favorite method of springing malware on victims, especially through Word and Excel. It's easy, with high chances of returns," said Amit Tambe, a researcher at F-Secure. "With one move, Microsoft tightened the noose on attackers."

Based on F-Secure's upstream data, attacks using OneNote documents have increased by a factor of three in 2023. However, cases of malware being spread through Word and Excel files have dwindled.

"We saw a 66% drop in the number of Word documents being used from Oct 2022 to Jan 2023," he said. "For Excel, there has been an even more significant drop—75%."

But who uses OneNote?

OneNote comes with both Windows 11 and Office 365. But the application is far less popular than Word or Excel.

"That's exactly why this attack is so effective," Tambe said. "Most people don't know what a .one file is. They figure they'll just click it and find out."

And Tambe said the product's near ubiquity puts average users at risk.

"OneNote supports the embedding of many other file types. This means attackers no longer need macros. They can simply attach the malicious payload inside OneNote file or embed URLs that point to malware. But only if you open them," Tambe concluded.

"Simply put, macros are—or were—attackers' favorite method of springing malware on victims."

Scams spike for Valentine's Day

F-Secure detected a significant rise in dating scams spread through spam as February 14th approached.

Junk email used to hook victims into dating scams is ever-present. But this threat spiked dramatically in the days leading up to Valentine's Day, according to F-Secure's monitoring of spam volume.

Playing with human emotions

"These criminals play with human emotions," said Patricia Dacuno, Senior Researcher at F-Secure. "And they know people may feel especially lonely around a day celebrating love."

Romance scams work in predictable ways, Dacuno noted.

"Criminals use fake or stolen photos to establish an attractive identity and build the fantasy of a romantic relationship," she said.

When the subject of meeting up comes up, the scammers offer excuses that include pleas for help paying for bills or travel. These requests continue until the victim can't or won't send more money."The final result is heartbreak and loss of money," Dacuno explained.

Broken hearts are big business

Almost 70,000 people reported being victimized by romance scam in 2022, according to the US Federal Trade Commission. The median loss was $4,400 and total losses equaled $1.3 billion.

"Reasonable thinking can easily be drowned out by loneliness," Dacuno said. "That's why it's invaluable to run quality Internet Security like F-Secure Total, which protects you from visiting suspicious dating sites."

But spam is far from the only way scammers carry out fraud. Many scams take place exclusively on social media platforms, such as Facebook.

"Scammers' biggest advantage is they play a numbers game and rely on proven tactics," Dacuno said. "Some of the profile pictures used in these scams circulating before Valentine's Day 2023 have been around since 2013."

Patricia Dacuno
Senior Researcher
Helsinki, Finland

expert tip

If anyone asks you for your bank account number or a money transfer, stop. Inspect the image of the person you think you're dealing with. It could be stolen or generated by artificial intelligence. Check the image for unusual distortions in the shapes and lines to see if it's fake or use Google Image Search to see if it's stolen. But if you're that suspicious, it's a good sign to break off all communication.

"Profile pictures used in these scams circulating before Valentine's Day 2023 have been around since 2013."

Breach reports

A selection of the month's biggest breaches, where confidential information has been exposed on the internet.

Local Gift Cards

Discovered: 16/2/2023

Affected people:
More than 148,000

Breach severity: ⚡⚡

Names, email addresses, usernames, passwords, and phone numbers appearing to belong to customers of Local Gift Cards, a U.S.-based ecommerce gift card store, were found on a hacking forum in early 2023. Anyone who has an account at localgiftcards.com should immediately change the password for that account and stop using that password—or any like that one—anywhere. In addition, closely monitor accounts that use that password for any suspicious behavior.

Weee!

Discovered: 16/2/2022

Affected people:
More than 1.6 million

Breach severity: ⚡⚡⚡

Email addresses of users of Gemini, a cryptocurrency exchange, were leaked on a hacking forum in late 2022. While this leak only involves emails, users should follow the best practice advice whenever data from a financial institution they use has been compromised. File a fraud alert with either Equifax, Experian, or Trans Union. Then check your credit to make sure your personal information has not been used to open any card you did not apply for yourself.

Truthfinder

Discovered: 2/9/2023

Affected people:
More than 7 million

Breach severity: ⚡⚡

Truthfinder is one of two services owned by PeopleConnect, a U.S.-based conglomerate that owns several sites that offer background checks on individuals, which seems to have recently suffered a breach. Names, email addresses, encrypted passwords, and phone numbers of customers of this subscription-based service appeared on a hacking forum in January 2023 and are now being shared across the internet.

Instant Checkmate

Discovered: 9/2/2022

Affected people:
More than 11.5 million

Breach severity: ⚡⚡

Instant Checkmate is the second service owned by PeopleConnect that reportedly suffered a breach of customer data. Customers should assume their password for this account has been comprised. This also offers a reminder that—when a company is breached—its other services may be affected, too. PeopleConnect reminded potential victims that it "will never ask you for your password, social security number or payment information via email or telephone."

Check out our **F-Secure Identity Theft Checker!**

Reddit reassures after breach

The popular social media platform reports no theft of user data after a successful phishing attack.

Joel Latto
Threat Advisor
Helsinki, Finland

expert tip

While you're going through Reddit's Safety & Privacy settings to enable two-factor authentication, make sure to uncheck all seven (yes, seven!) privacy-infringing options that would offer you personalized ads and allow search engines to link to your profile in their search results.

"You should change your password after a data breach notification."

An employee of Reddit—one the internet's favorite sites for sharing and consuming news, humor, and opinions—fell for a phishing attack in early February, which allowed criminals to steal internal documents, data, and source code.

In a statement on the site, the company reported that "several days" of investigation had revealed that the stolen data affected current and former employees along with some advertisers, but no users.

ZDNet credited Reddit for the site's "transparent response." Joel Latto, F-Secure Security Advisor, echoed praise for the disclosure, noting it came only four days after the breach was discovered and was described in terms the average Redditor could understand.

It wouldn't be the first time.

But Latto also offered a reminder that quick assurances after breaches don't always pan out. "It wouldn't be the first time a company rushes to assure its customers or users that their data is safe, before finishing a thorough investigation of what the threat actor has done," he said. "Sometimes the extent of the breach might be discovered only after a couple of weeks."

Latto also agrees with the site's advice to activate two-factor authentication.

Change your password?

However, Reddit's advice to periodically change passwords is "outdated" and hasn't been recommended by NIST (The National Institute of Standards and Technology) for the past six years.

"But you should change your password after a data breach notification—whether or not the company in question thinks your account has been compromised."

So, change those Reddit passwords now—if you haven't already.

Vastaamo suspect arrested

Man accused of extorting psychotherapy patients was convicted of over 50,000 crimes related to hacking as a youth.

Julius “Zeekill” Kivimäki faces extradition to Finland from France to face eight charges related to the hacking, extortion and leaking of the mental health records of over 30,000 patients from the (now bankrupt) Vastaamo Psychotherapy Center.

Laura Kankaala, F-Secure’s Threat Intelligence Lead, called th e Vastaamo story a “tragedy” that’s “a cautionary tale about corporations trusted with sensitive data and young people who fall into increasingly risky online behavior.”

Not if, but when

Vastaamo stored patient information, including notes from hundreds of thousands psychotherapy sessions, on a database open to the internet that was secured just a default password.

“Accessing such a database doesn’t require a lot of technical knowledge or skills,” said Kankaala. “If a company has an unprotected database, compromise of it is not a matter ‘if.’ The question is ‘When?’”

When Vastaamo refused to pay a ransom, the company’s data was breached, and the criminal then sent extortion demands directly to patients. However, most of the victims rejected the demands. At which point the criminal retaliated by leaking all the patient data online.

In 2015, long before the Vasataamo breaches began, Kivimäki, then aged 17, received a four-figure fine after being convicted of over 50,000 crimes, including breaches, fraud, and bomb threats. And Kankaala noted that, whilst the crimes Kivimäki stands accused of related to Vastaamo occurred when he was an adult, the warning signs were already there.

“It’s hard to not see this story as the system failing to prevent a disturbed young man from falling deeper and deeper into crime,” Kankaala said.

A 2022 study from the Institute for Connected Communities found that two thirds of young Europeans aged 16-19 (69%) now engage in some form of online risk taking or cyber crime, ranging from spamming to sextortion to cyber bullying and hacking.

Laura Kankaala
Threat Intelligence Lead
Helsinki, Finland

expert tip

Whatever is online can never be deleted. Some of our data, like compromised passwords, is easy to change. Other information, such as patient records, cannot be changed. In tragic cases when someone threatens or bullies you based on your breached private information, the best advice is to take it as seriously as possible. File a police report and seek counselling, if needed.

“If a company has an unprotected database, compromise of it is not a matter ‘if.’ The question is ‘When?’”

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 170 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 today!

F-Secure