F-Alert

Monthly threat updates from

F-Secure

May 2023

F-Secure

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

Learn how Google, Apple, and Microsoft want to get rid of passwords. Find out about the nation-state attackers who may target you on Facebook. Discover what LGBTQ+ users need to know for a safer Pride. And learn how to spot faked images generated by AI in this month's F-Alert.

Google rolls out passkeys

The end of passwords has been predicted for years, and Google, Apple, and Microsoft are trying to make that happen sooner than later.

Google took a giant step toward a "passwordless future" with the rollout of passkeys in early May.

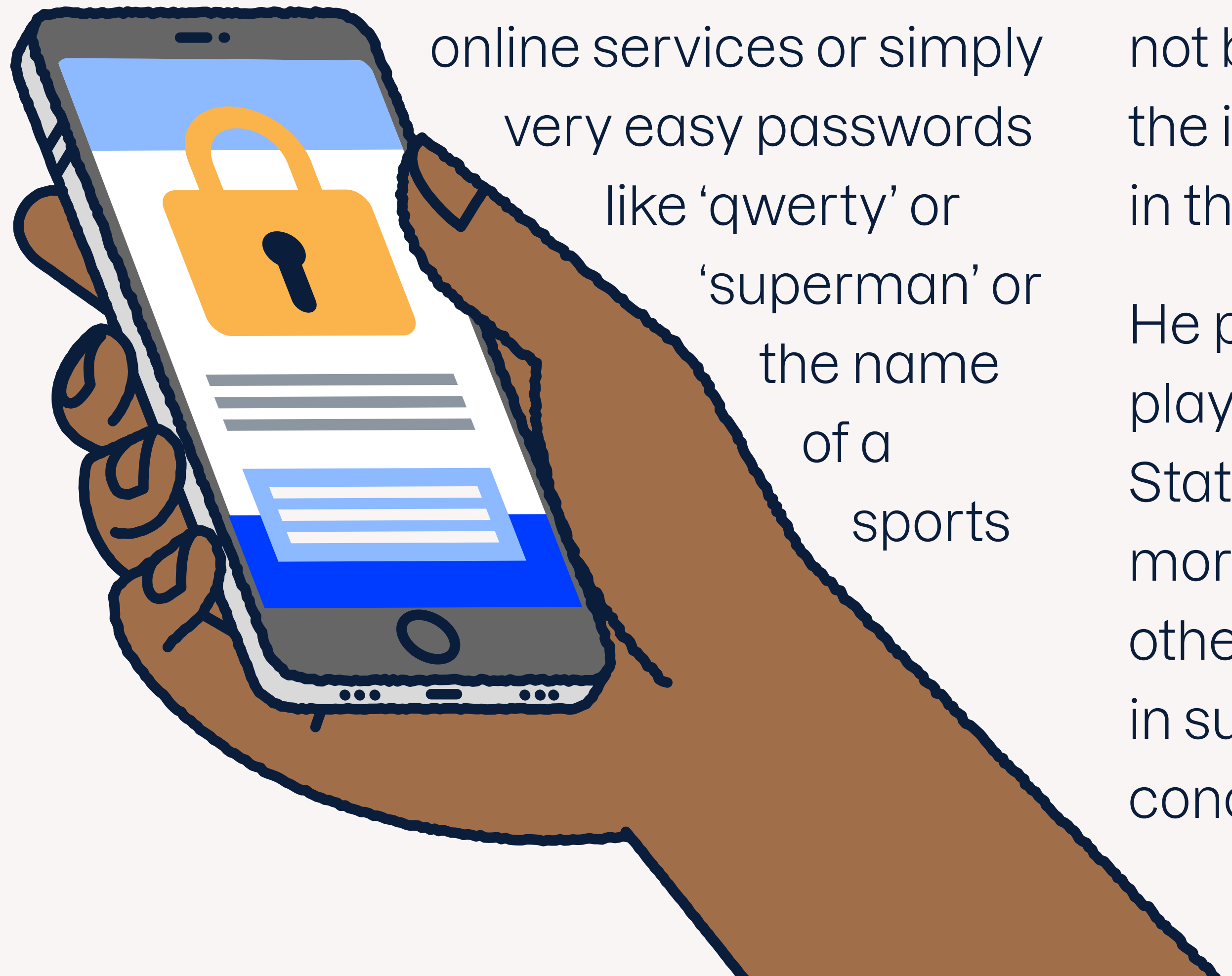
Passkeys are digital credentials that aim to replace passwords by adding a new layer of security that connects user accounts to websites or apps, across platforms and devices. They allow people to verify themselves with a fingerprint, a face scan, or a screen lock PIN. And even if passkeys are somehow breached, they only work on the account owner's device.

A real consumer pain

The movement toward replacing passwords has been propelled by a consortium called the FIDO Alliance backed by the world's largest search company along with fellow tech giants Apple and Microsoft.

"It is very positive to see that these ecosystem owners try to address a real consumer pain and a real security risk related to creating and using passwords properly," said Timo Salmi, F-Secure Senior Solution Marketing Manager, who has spent years working on solutions that help users secure their accounts.

The burden on consumers to create credentials that authenticate several if not dozens of services can lead to cutting corners, Timo noted.



"A typical mistake is to use the same password in multiple online services or simply very easy passwords like 'qwerty' or 'superman' or the name of a sports team," he said. "Data breaches often reveal that the most common password on the internet is… 'password'".

Gatekeepers of the internet

Timo hopes that this step from Google is the beginning of a global movement.

"It is unfortunate that we are missing large European ecosystem providers like Google, Apple, and Microsoft. If Google, Apple, and Microsoft have not been seen as the gatekeepers of the internet before, they will soon be in that role – literally," he said.

He pointed out that all these key players come from the United States. "It would be positive to see more active participation also from other regions like Europe and Asia in such fundamental initiatives," he concluded.

Timo Salmi
Senior Solution
Marketing Manager
Oulu, Finland

expert tip

It will take years for passwords to disappear. While waiting for the next wave in authentication it is important to remember good password safety by creating strong and unique passwords and storing them properly, ideally in a quality password manager like the one included in F-Secure Total.

> **"Data breaches often reveal that the most common password on the internet is… 'password'."**

Hoai Duc Nguyen
Researcher
Helsinki, Finland

expert tip

Meta Work accounts that allow users to manage business accounts without logging into a personal account are coming later this year. Until then, avoid personal activity on accounts that you use for business purposes.

> “That’s how a consumer threat quickly becomes an enterprise threat.”

Meta takes on advanced threats

Users of the world’s largest social network face threats and manipulation from advanced attackers often backed by nation states.

A new report from Meta offers growing evidence that extremely well-resourced criminals continue to escalate their activities on Facebook, targeting business accounts and manipulating public opinion.

Gain trust and install malware

Meta reported removing three Advanced Persistent Threat (APT) groups from Facebook in the first quarter of 2023. APTs are generally state-backed or sponsored organizations known for their patience, stealth, and relentlessness.

“All three networks of these networks heavily employ social engineering,” said Hoai Duc Nguyen, a researcher at F-Secure. “That means they use psychological manipulation to trick users into making mistakes.”

These efforts require resource-intensive investment in creating fake accounts, websites, and personas. Attackers often pose as recruiters who toy with users’ desires for career advancement.

“The goal is to gain a victim’s trust and then install malware that hijacks a company’s Facebook business account,” Nguyen said. “That’s how a consumer threat quickly becomes an enterprise threat.”

That’s why Meta has rolled out several new ways to protect business accounts from malware.

Coordinated manipulation is also a crime

Meta also removed six networks that reportedly engage in coordinated inauthentic behavior (CIB).

This attempt to manipulate consumers’ minds with the mass sharing of propaganda through a wide variety of individual Facebook accounts is less personally intrusive than account hijacking.

But it’s still a crime, Nguyen noted.

“These manipulators hide their activities behind fake identities to create the sense of an organic political movement.”

Distinguishing coordinated activities from genuine political movements presents a unique challenge.

“The differences between an individual acting with blind faith and a fake account being weaponized for misinformation can be difficult, if not impossible, to detect,” Nguyen concluded.

Trending Sc@m

Phishing campaigns using the popular discount brand **Shein** are actively spreading in multiple languages across Instagram.

This fraud utilizes one of Instagram's most popular features. Scammers attract victims by tagging users in the comments of the post. The endpoint of the attack is a phishing site that ultimately steals credit card information.

Victims of this scam should immediately contact their financial institutions to check for fraudulent payments and cancel any affected credit cards.

Breach that matters

Stolen private data from two dating sites—**CityJerks** and **TruckerSucker**—we identified on a criminal hacker forum in late April.

The breached data includes usernames, email addresses, passwords, profile pictures, sexual orientation, users' date of birth, their city and state, their IP addresses, and biographies, along with private direct messages—which are especially sensitive given the nature of the sites.

Potential victims should immediately change any passwords or usernames—or variations on those—that may have been used on the sites. In addition, users of dating sites should establish unique email addresses to use for these services along with the unique usernames and passwords—and these credentials should have no connection to any accounts used for work or professional or financial endeavors.

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

Infostealers in the wild

Shedding light on a growing cyber security issue – the rise of the infostealer

An infostealer is malware designed to steal important information from your browsers and more. Here, we've ranked infostealers by most stolen records discovered in April:

Raccoon	16,551,337
Redline	9,354,919
stealc	549,537
Vidar	489,992
MetaStealer	284,678
Aurora	98,952
Darklord	35,431
LummaC2	24,705
Taurus	13,220
Dark Crystal	6,289
Hunter	3,325
Ebrium	1,972
Ghostbuster	1,460
Rhadamanthys	1,344
Atlantida	393
Titan	43
Mars	41

A closer look at

REDLINE
INFOSTEALER

This infostealer steals data from infected computers. It can be purchased online and is advertised on many of the popular online marketplaces where hacking tools and data dumps are being sold, or for example Telegram channels.

This infostealer can swipe:

Logins and passwords | Session cookies | Autocomplete fields, such as credit card information | Data from instant messaging applications such as Discords | Information about the victim's system, such as IP address, location and operating system information

Redline stealer infections have originated from:

Software vulnerabilities | Fake game hacks | Fake update installers and other fake applications | Targeted phishing attacks

How to detect AI images

AI image generators create incredibly realistic fake images in seconds and the technology will only get better.

Believable fake digital images have littered the internet for decades, but increasingly powerful image generators like Midjourney, DALL-E, and Stable Diffusion can now create convincing fakes in seconds.

Weaponized fakes

The upsides of these creative tools come with significant opportunities for misuse, said Laura Kankaala, F-Secure's Threat Intelligence Lead.

"You probably saw the AI image of the Pope in a cool puffer jacket that crisscrossed the internet in March," she said. "But the same technology that brought so many people a smile could also be weaponized for romance scams, phishing, disinformation, and fraud of all sorts."

In seconds, criminals can create an array of fictional images that could show up in a dating profile, an ad for a questionable product, or a plea for a charity that doesn't exist.

"Often fake images have been stolen from someone else's social media." she said. "But the problem with machine-generated images is that it becomes essentially impossible to do any sort of reverse image search for them, as you can with stolen images."

What to look for

Laura noted that there are some subtle hints that the image you're looking at may be faked either by an AI generator or an "old school" image editing tool, such as Photoshop.

These hints include rounded edges, fuzzy eyes, strange-looking features, like pointy ears or too many or too few fingers, a spooky glow, or a background that is unclear, fuzzy or blurred, and containing weird glitches. However, these telltale signs will be gone once generative AI technology improves further. In some cases, it may already be impossible to tell a fake from real without analyzing the context.

Laura noted that the best way to combat fake images, especially those possibly associated with scams, is to analyze the context and what kind of engagement you have with the person using the suspicious images.

"Is the person you're talking to online suddenly asking for money or investment? Are they trying to make you download something? Are they scaring you into doing something that relates to money or purchasing something?" she said.

Laura Kankaala
Threat Intelligence
Lead
Helsinki, Finland

expert tip

Since generative AI is advancing so quickly, it's more important than ever to make sure to use strong passwords and multi-factor authentication to protect your accounts from potential scammers. It's also important to proactively protect devices from malware with endpoint protection, as scammers could try to get access to your data via a malicious program.

"Are they scaring you into doing something that relates to money?"

Fennel Aurora
Product Management
Community Lead
Paris, France

expert tip

Beware using your phone in a country that is fully intercepting data traffic. The fact that you are sending traffic to an LGBTQ+ dating app, such as Grindr, is visible, unless you are using a VPN — and in some of the same countries VPNs may well be blocked in that country or using one may result in unwanted police attention.

> **“Many LGBTQ+ people face the risk of being fired, with little recourse.”**

LGBTQ+ people deserve privacy

Pride month offers an annual reminder that even data collection with best intentions presents unique risks for LGBTQ+ internet users.

For LGBTQ+ people across the globe, privacy can be a matter of life and death.

“Security advice that does not consider both the vital necessity for LGBTQ+ people to hide their identity in many situations and the psychological toll this necessity takes, puts about 10% of the population in danger,” said Fennel Aurora, F-Secure’s Product Management Community Lead.

Data collection—a necessary evil?

One example that shows how even efforts to increase equitable treatment for people of all genders and sexual orientations comes from the United States, where the Biden administration is attempting to collect more data on LGBTQ+ citizens to increase access to essential services.

“Given the regressive political atmosphere across much of the country, activists are rightly raising concerns that this data could be used to endanger the people this collection is designed to help,” Aurora said. “Many LGBTQ+ people face the risk of being fired or not hired, with little recourse. Why should they offer their private information to a revolving government that may persecute them?”

So much to consider

While Pride is a time to proudly celebrate progress, equity and opportunity, the excessive burdens LGBTQ+ internet users face can’t be ignored.

Aurora offered a variety of questions these users face about their online activity that others are rarely forced to consider. “Do you tag your location on your social media posts? What about that post last night from a queer nightclub? Are you sure you trust everyone who can see your posts?”

And that’s just the beginning, especially for younger people who face not only the scrutiny of society but their own families, who may or may not be supportive of their exploring their sexuality or gender.

“The LGBTQ+ community faces higher risks of homelessness and a higher percentage turning to more dangerous forms of sex work,” Aurora said. “While the internet offers freedom that didn’t exist a generation ago, it hasn’t erased these sad realities.”

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®