F-Alert

Monthly threat updates from

F-Secure

October 2023

F-Secure

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

Find out the hidden danger behind some QR codes. See why Google wants you to forget your passwords. Discover what your cheap Android TV device may be doing while you're watching Netflix. And learn why most shopping scams start with Facebook ads. All this and more in this month's F-Alert.

Joel Latto
Threat Advisor
Helsinki, Finland

expert tip

It's great that iOS, for example, shows a link preview when reading a QR code. But it only shows a partial link. You still need browsing protection to protect against the bad URLs that QR codes may trigger.

"QR codes can circumvent spam protection easier than regular phishing."

QR phishing goes mainstream

Attacks using QR codes to steal credentials have gotten so common that they now have a nickname—quishing.

The first QR or "quick response" codes were designed in 1994. But they didn't become familiar to many internet users until recently, when the technology was adopted by leading two-factor authentication apps and as a touchless digital tool during the Covid-19 pandemic.

Cyber criminals, of course, never miss an opportunity. In October of 2023, AT&T warned about "quishing" attacks as searches for "QR code phishing" hit record highs.

A somewhat unique threat

Some cyber security pros are debating if "quishing" exists or if it's just a too-cute way of describing another form of phishing, one of most common threats that users face.

But there are unique aspects to threats that arise from scanning codes that consumers need to be aware of, explained Joel Latto, F-Secure Threat Advisor.

"QR codes can circumvent spam protection easier than regular phishing, since the email itself doesn't need to have any outbound links that might trigger detection," he said. "They can also be used to initiate a download of a malicious app or file, especially on phones."

In the wild

QR code scams are also unique in that users can also come across them when both online and off, added Latto, who has been warning about the dangers of QR codes "in the wild" for years.

Last year, the FTC warned consumers about a scam in Texas that began with malicious QR codes on parking meters.

"Really the only limit here is criminals' imaginations," he concluded.

Trending Scam

“Phantom Hacker” wipes seniors out

WHAT:
The FBI has warned about a three-phase scam that has claimed more than half a billion dollars in losses in the first half of 2023 alone, often by targeting senior citizens and taking everything they have. This fraud resembles a traditional tech support scam and develops into criminals posing as banking or government officials who insist victims transfer large sums of money to various accounts for “safe” keeping.

HOW:
Using the knowledge of the financial accounts that the victim has accessed through the machine, the criminals make specific demands for funds to be sent overseas via wire transfer, cash, or cryptocurrency while insisting the transactions be kept secret.

PREPARE:
1) Never give in to a request to download software from anyone who has contacted you and 2) immediately stop and seek assistance if a stranger tells you not to tell anyone about what they’re asking you to do.

Breach that matters

23andMe

WHY IT MATTERS:
User data from at least 835,000 23andMe customers appeared on an online forum in early October. The genetics testing site has confirmed that its “DNA Relatives” offering has been “impacted”.

BREACHED DATA:
The data contains names, birth dates, country, email addresses and other personal information. What’s unique about this leak is the data has reportedly been identified and grouped by ethnicity—specifically Ashkenazi Jews and Chinese descent.

WHAT SHOULD YOU DO:
All users of 23andMe should make sure their password is strong and unique and activate two-factor authentication. The EFF suggests users may want to download their data from the site and delete their accounts or at least consider the implications of trusting a third-party with data relating to DNA, which contains all your genetic information.

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

Google pushes passkeys

The tech giant now encourages all users to ditch passwords in favor of a fingerprint, face scan, pin, or pattern.

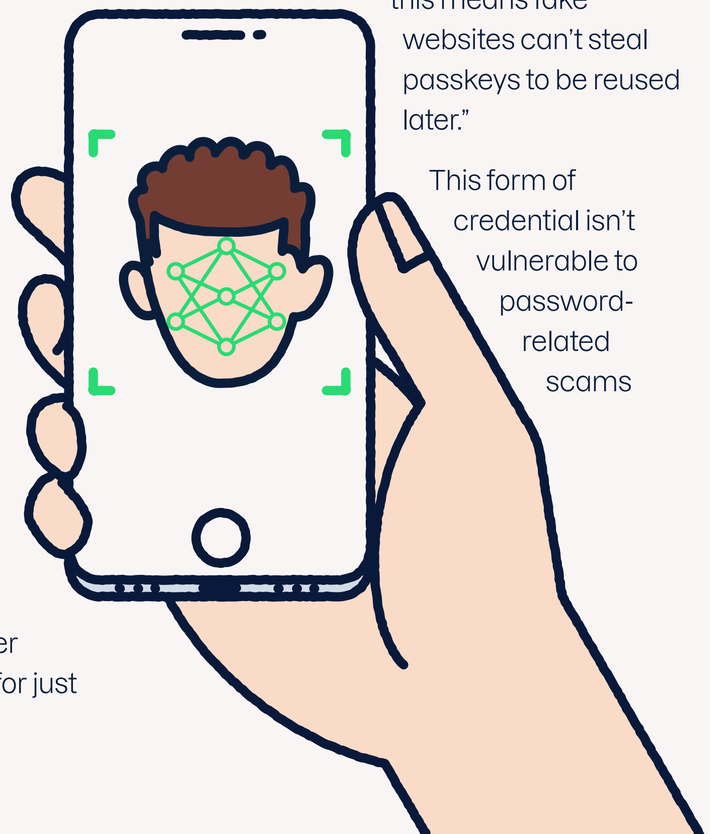
They're more secure than passwords. You don't need to remember them. And they're 40% faster.

That's Google's argument for why passkeys have now replaced passwords as the default for securing accounts on the platform. This step marking Cybersecurity Awareness Month is the latest sign that industry leaders continue to be serious about ending the era of the password.

Cannot be reused

Ash Shatrieh, F-Secure Threat Intelligence Researcher, investigated the passkey protocol and agrees that they're a better option than passwords—for just about every reason.

"Users can use passkeys to log in to websites or apps simply by using a device's biometric authentication, such as a fingerprint or face scan" he said. "Passkeys are website-bound; this means fake websites can't steal passkeys to be reused later."



This form of credential isn't vulnerable to password-related scams fueled by constant data breaches or phishing.

Numerous benefits, but not perfection

"The shift towards a passwordless world offers numerous security benefits, but it's not yet perfect," Ash said. "The way passkeys must sync into the user's cloud means the account recovery process is still open to phishing attacks."

Google had implemented passkeys as part of the FIDO alliance effort to eliminate passwords earlier this year. Many FIDO members - including Amazon, Apple, and Microsoft - have already implemented passkeys support.

"When the largest search and ad company on earth makes something default, others tend to follow," Ash concluded.

Ash Shatrieh
Threat Intelligence Researcher
Helsinki, Finland

expert tip

The threat landscape will shift towards account recovery phishing rather than being fully eliminated. The security of users' identities remains as good as their accounts' recovery processes.

"The shift towards a passwordless world offers numerous security benefits, but it's not yet perfect."

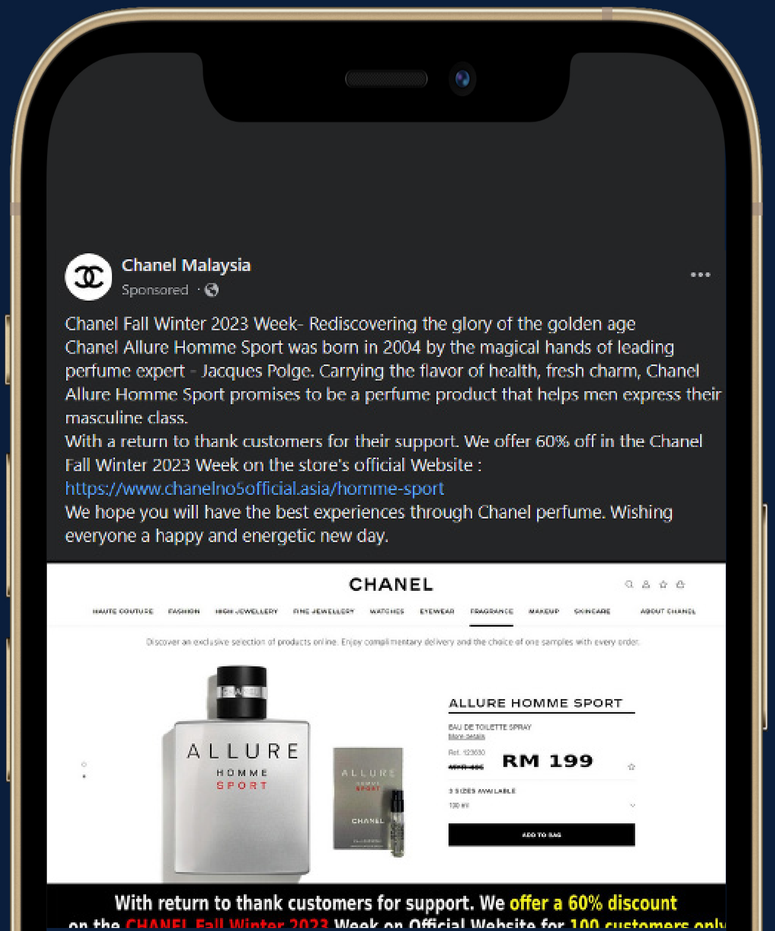
How Facebook shopping scams work

Shopping scams are on the rise thanks to social media platforms pushing almost anything as ads.

If you're going to lose money from a scam, chances are that scam will start on social media.

And if you're going to be scammed on social media, one big reason is that these platforms are filled with advertisements showing fake products with fake discounts.

44% of all social media fraud loss reports came from people who tried to buy something being advertised on social media. Similar to this:

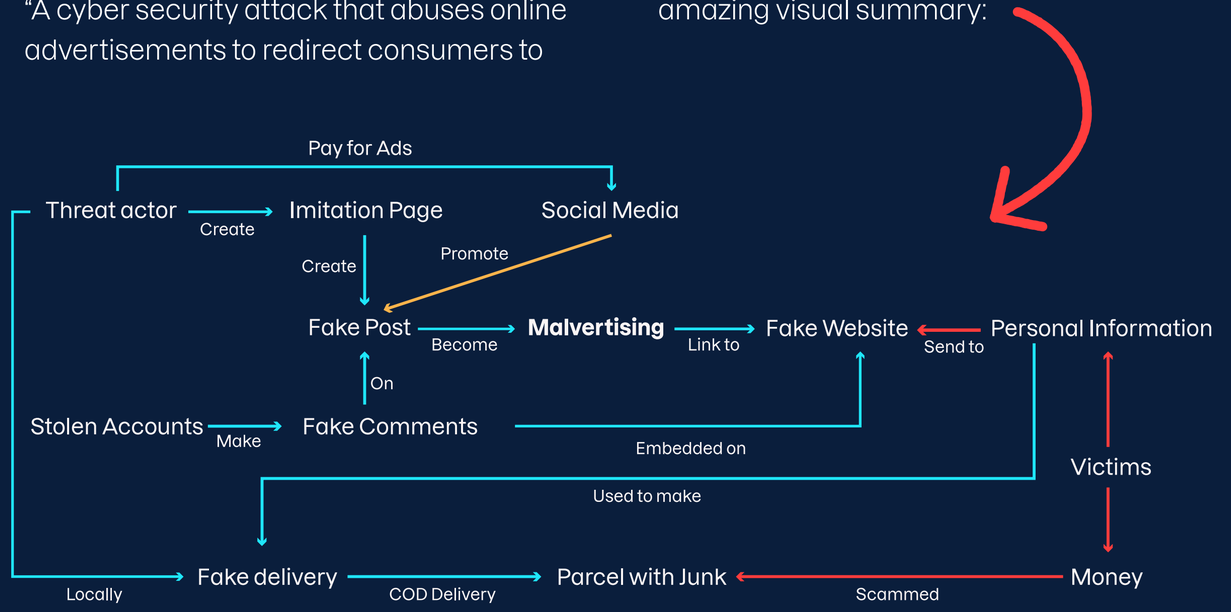


The most common shopping scams ended with the purchased goods never arriving or arriving switched out with junk.

This sort of scam employs Malvertising. What's that?

"A cyber security attack that abuses online advertisements to redirect consumers to malicious websites and applications," said Yik Han, a researcher at F-Secure, who found the example above.

We asked Yik Han for an introduction into how this cyber crime has become a billion-dollar business. He came up with this amazing visual summary:



The short version?

Bad folk set up fake Facebook pages imitating brands that you like. They then create fake posts that get promoted as ads and further boosted with fake comments. These then link to fake websites that pressure you into buying something that will never arrive.

Yik Han
Researcher
Puchong, Malaysia

expert tip

"It is easy to fake everything on social media nowadays. So be sure to check if the online seller is legitimate with a tool like F-Secure's Online Shopping Checker before you make any purchase."

Android TV backdoors exploited

Popular streaming devices installed with malware seem to be carrying out fraud.

Mika Lehtinen
Director of Research Collaboration
Helsinki, Finland

expert tip

When shopping for Android hardware, look closely at recent reviews and try to stick to Play Protect–certified devices. None of the affected boxes were certified by Play Protect.

“The mystery is when the backdoors in the firmware were installed.”

A report earlier this year found Android TV boxes from Chinese manufacturers may come installed with active malware. Now, new evidence suggests that devices from hundreds of Android models have been enlisted in a network of zombie devices to commit fraud.

Sold on mainstream sites

“The report identified 77,000 devices with backdoors that open them up to malware installation, but there are probably millions of these boxes sold globally,” said Mika Lehtinen, F-Secure’s Director of Research Collaboration. “Millions of similar machines are on the market.”

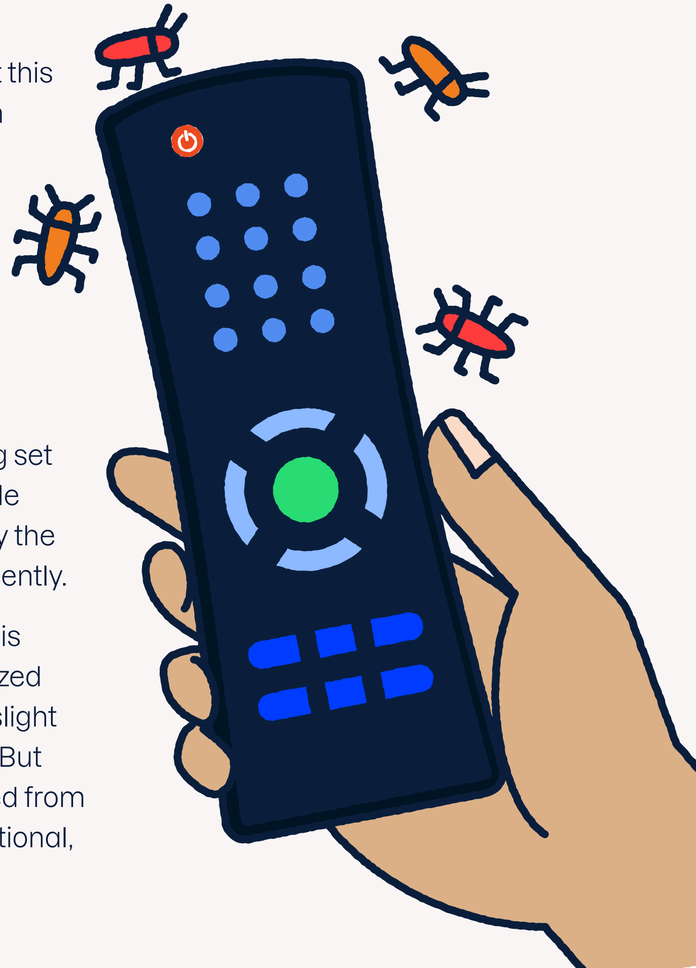
Affected models were delivered to customers infected with a sophisticated and adaptable malware known as Triada that received active fraud “modules” as soon as the devices were powered up.

“What’s most significant is that this hardware is being sold through mainstream ecommerce sites like Amazon,” Lehtinen said. “The mystery is when the backdoors in the firmware were installed.”

Customers in the dark

The ad fraud, fake emails being set up and hijacked proxy, and code installation being carried out by the infected boxes all take place silently.

“The only sign that your device is participating in a global organized crime botnet may come from slight performance issues,” he said. “But since these devices are infected from the moment that they’re operational, the chances of a customer picking up on this are tiny.”



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