FORBES > INNOVATION > CYBERSECURITY

FBI Warns Gmail, Outlook, AOL And Yahoo Users—Hackers Gain Access To Accounts

Zak Doffman Contributor
Zak Doffman writes about security, surveillance and privacy.

Follow

9

Nov 3, 2024, 05:38am EST

Updated Nov 5, 2024, 02:01pm EST

FBI issues new warning for Gmail, Outlook, webmail users NURPHOTO VIA GETTY IMAGES

Updated on November 3 with new reports into passkey adoption as alternative to MFA, with new updates to widen take-up further, resolving key challenges.

"Cybercriminals are gaining access to email accounts," the FBI warned this week, even when accounts are protected by multifactor authentication (MFA). Attacks begin when users are lured into "visiting suspicious websites

or click on phishing links that download malicious software onto their computer."

Email access itself comes by way of cookie theft. Not the devilish tracking cookies that we read so much about, and which caused havoc when Google reversed its promise to eradicate them from Chrome. These are session cookies or security cookies or "remember me" cookies. They store credentials to stop you having to log in every time you visit a website or access one of your accounts.

FORBES

Google Issues Cookie Theft Warning—But Has A Clever New Fix

By **Zak Doffman**

The threat affects all email platforms providing web logins, albeit Gmail, Outlook, Yahoo and AOL are by far the largest. The same threat clearly impacts other accounts as well, including shopping sites and financial platforms, albeit there are now often additional protections in place, especially with financial accounts. MFA is not usually stored in the same way, and criminals use other means to steal live codes.

"Many users across the web are victimized by cookie theft malware," Google has warned, "giving attackers access to their web accounts." While "fundamental to the modern web… due to their powerful utility," Google describes security cookies as "a lucrative target for attackers," and that problem is getting worse.

MORE FROM FORBES ADVISOR

Best High-Yield Savings Accounts Of 2024

By **Kevin Payne** Contributor

"Typically, this type of cookie is generated when a user clicks the 'Remember this device' checkbox when logging in to a website," the FBI explains. "If a cybercriminal obtains the Remember-Me cookie from a user's recent login to their web email, they can use that cookie to sign-in as the user without needing their username, password, or multifactor authentication (MFA)."

Cookie theft has been much in the news recently, with ongoing efforts from Google and others to prevent such thefts from Chrome and other browsers. These latest such initiatives focus on linking cookies to devices and apps, rendering thefts useless. But we're at an early stage and cookie theft remains a major threat.

"Cybercriminals are increasingly focused on stealing Remember-Me cookies and using them as their preferred way of accessing a victim's email," the FBI warns, but provides four suggested actions "to protect yourself from putting yourself at risk:

- Regularly clear your cookies from your Internet browser.

- Recognize the risks of clicking the 'Remember Me' checkbox when logging into a website.
- Do not click on suspicious links or websites. Only visit sites with a secure connection (HTTPS) to protect your data from being intercepted during transmission.
- Periodically monitor the recent device login history from your account settings."

As ever, if you think you may have fallen victim to this or any other cybercrime, you can report it to the FBI's Internet Crime Complaint Center (IC3) at www.ic3.gov.

The FBI's latest warning on MFA compromises should in no way discourage any users from setting MFA up on all accounts where it's available. It is the single best step you can take to secure your accounts. And allied with good housekeeping on what you download, install, click and open, it can keep your safe.

The importance of MFA has been neatly summed up with the response to Amazon finally adding MFA to its enterprise email service. "Better late than never appears to be the justification behind the near-decade delay," reported *TechRadar* on Friday, "especially for one of the most basic forms of identity verification that has been standard practice for several years now," warning "there are still hurdles to enabling MFA for WorkMail, as it will not be enabled by default and system administrators will have to manually add each user to the AWS Identity Center."

FORBES

Why You Should Buy A New Microsoft Windows PC In 2025

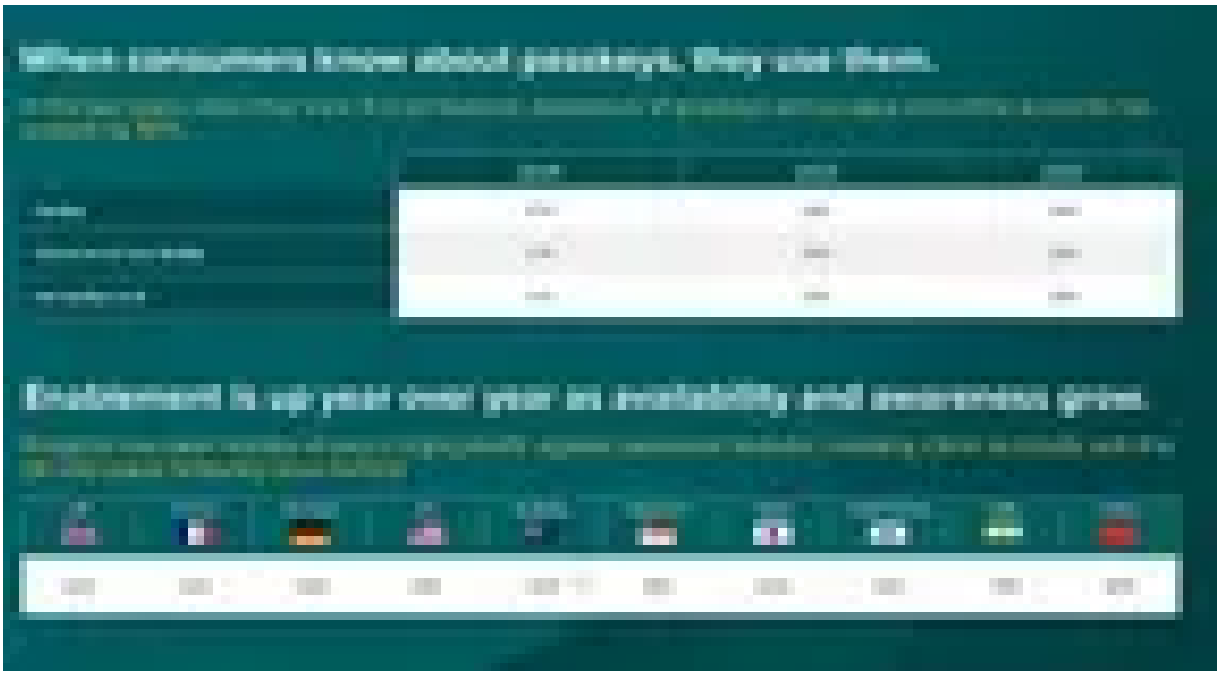
By **Zak Doffman**

The Register echoed this sentiment. “The fact that a security service as simple as MFA was missing from something that so desperately needs it - an enterprise email platform run by one of the biggest (if not *the* biggest) cloud services providers in the world - is shocking, frankly.”

Any MFA is better than none—period. But there is clearly a spectrum of security, and not all solutions are the same. Passkeys are best when available—they link credentials to device security, akin to a physical security key without the hassle of using an actual physical security key. But if all you have available is an SMS one-time code, then using that is better than leaving your security password only—every time.

The good news for users is that passkeys are catching fire. According to a new report from the FIDO Alliance, “in the two years since passkeys were announced and made available for consumer use, passkey awareness has risen by 50%, from 39% familiar in 2022 to 57% in 2024.” Passkeys are far and away the easiest alternative to the combination of a username and password and the MFA you should always use when available. They stop unauthorized access to an account unless an attacker has full control over one of your secure devices, essentially purporting to be you.

“The majority of those familiar with passkeys are enabling the technology to sign in,” FIDA says. “Meanwhile, despite passwords remaining the most common way for account sign-in, usage overall has declined as alternatives rise in availability.”



The surge in passkey adoption FIDO

Putting aide the security benefits of passkeys, FIDO also points out the benefits to brands and services platforms that now offer this as an option. “42% of people have abandoned a purchase at least once in the past month because they could not remember their password,” it says, adding that “this increases to 50% for those aged 25- 34 versus just 17% for over 65s,” which raises a different issue.

Echoing the FBI warning, FIDO also says that “over half of consumers reported an increase in the number of suspicious messages they notice and an increase in scam sophistication, driven by AI. Younger generations are even more likely to agree, while older generations remain unsure how AI impacts their online security.”

FIDO’s new report shows passkey take-up is highest where linked to the ease of biometric device security. This seamless approach to securing one’s identity is the same driver behind the viral rise in Apple Pay, Google Pay and other digital wallets.

While passkeys are primarily aimed at the consumer/home market, moves are now afoot to extend this into enterprises. As *9to5mac* has just reported, “the FIDO Alliance has taken a big step toward improving the usability of

passkeys by introducing two new draft specs: the Credential Exchange Protocol (CXP) and the Credential Exchange Format (CXF). These proposals are designed to solve a key issue slowing the adoption of passkeys in the enterprise: vendor lock-in."

FORBES

New Microsoft Windows Attacks—Stop Doing This Now, US Government Warns Users

By **Zak Doffman**

These new specifications should create a "standardized, secure way to transfer passkeys between different password managers without removing and re-adding from each platform," which matters more for enterprises than users already locked into their iPhone, Android or password manager ecosystem.

"By standardizing how passkeys are managed and transferred," *9to5mac* suggests, "the new specifications will help businesses and consumers have more freedom in choosing the best tools for their needs without being locked into a single ecosystem. Over time, this will drive broader adoption of passkeys, further pushing the shift away from passwords, often the weakest link in personal and organizational security."

Follow me on Twitter or LinkedIn.

Zak Doffman

Follow

Zak Doffman has covered security, surveillance and privacy on... **Read More**

Editorial Standards

Forbes Accolades