How Hackers Are Stepping Up Phishing Attacks (and How to Fight Back)

The cyber landscape has come a long way from the days when foreign princes emailed us, offering to wire us money, if only we shared our bank account information. Unfortunately, after all these years, such phishing attacks remain one of the most persistent threats to an agency's cyber defenses.

And the problem is stickier than you might realize. One of the best defenses against phishing is multifactor authentication (MFA), which requires users to provide something more than a password, such as a biometric scan, a one-time code or an email notification. Sadly, traditional MFA is not as foolproof as people like to think.

That conundrum was the focus of a recent GovLoop virtual event titled "The Truth About Phishing in Gov." The event was sponsored by Okta, which provides identity and access management solutions.

Here are some takeaways from the session.

Modern Phishing Finds Its Marks

These days, phishing is less focused on stealing from individuals and more on cracking the defenses of large organizations by luring employees into sharing passwords or downloading malicious code.

And those phishing attempts are more sophisticated than ever. The emails lack the telltale grammatical errors and typos, and the designs are nearly indistinguishable from whatever senders are being spoofed. AI chatbots only make it worse.

"It's very hard for a user to look at those and say, 'This is a legitimate email, and this is a phishing email,' because the fidelity is so good," said Sean Frazier, Federal Chief Security Officer at Okta. "You really have to be a forensic scientist to figure out the differences."

Phishing attempts are also coming through other channels (i.e., attack vectors), such as LinkedIn, SMS text or direct messaging, he added.

Simply put, organizations cannot continue to rely on employees to repel those attacks, said Steve Caimi, Cyber Specialist for Public Sector at Okta.

"We have to remove the burden of cyber diligence from the users," he said. "At this point, there's no way that people can stay vigilant, especially with all the different vectors."

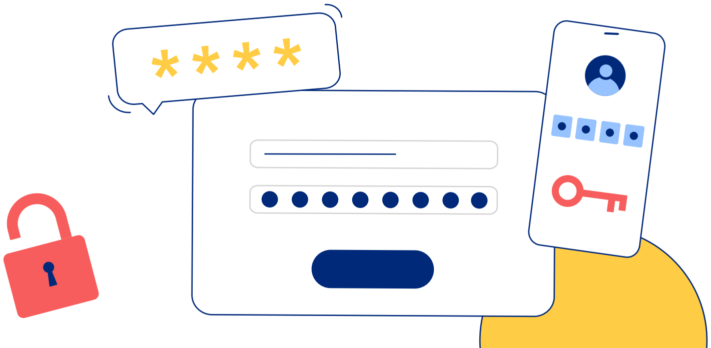
Traditional MFA Only Goes So Far

Make no mistake: Multifactor authentication, or MFA, represents a big leap over the use of passwords. Over the years, cyber criminals have proven to be increasingly adept at cracking passwords, either by stealing them, getting users to share them or just guessing them ("password" still being a common password).

With MFA, a hacker who snares a password still needs that other factor, such as a one-time password or text message, before they can do anything with it. That raises the barrier to entry.

But MFA, while an improvement, was only a stopgap measure, Frazier said. The problem is that MFA can be circumvented. You can "phish the factor," e.g., get users to share a one-time password or click on a phony push notification.

More recently, Okta has seen a rise in adversary-in-the-middle attacks. In this scenario, a hacker hijacks a user session and redirects the traffic to an impersonated web application. If the user is fooled and signs in, the hacker captures those credentials and gets to work.



Next Up: Phishing-Resistant MFA

The key to making MFA phishing resistant is what's known as binding.

Again, in traditional MFA, a user is granted access to an application or another resource once they provide the required factors, such as a password and push notification. Phishing-resistant MFA raises the bar by requiring a user to authenticate for a given website or application using a specific device.

In short, for the purpose of authentication, a person's identity is bound up inextricably with the site or resource being accessed, the multiple factors being submitted and the device being used. For hackers, stolen credentials no longer will suffice.

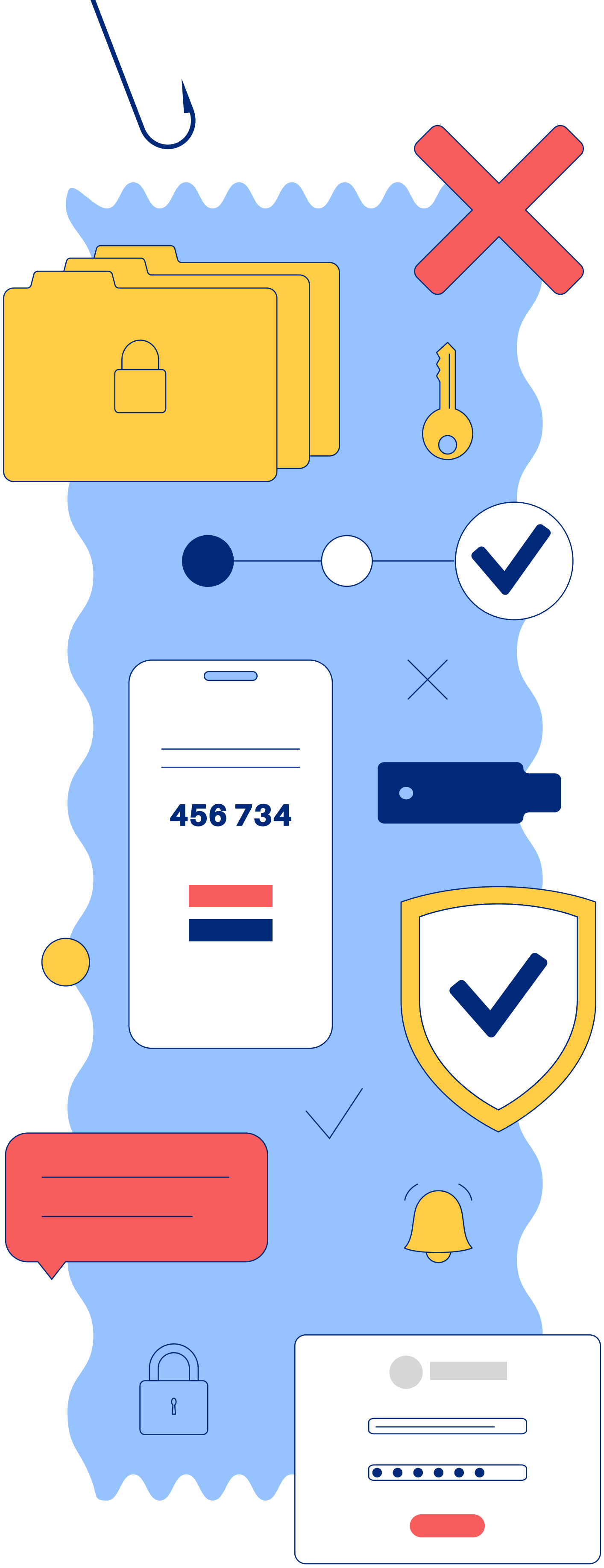
The trick, of course, is raising the barrier of entry for hackers without doing so for employees. That's the idea behind passkey technology.

A passkey, based on industry standards set by the FIDO (Fast Identity Online) Alliance, is a password-free digital credential that is tied to a user and that user's device or devices. As long as a user is using an enrolled device, they will be authenticated automatically when accessing an application. Organizations can incorporate a biometric scan or another factor as an additional layer of security.

Okta FastPass provides agencies with the tools they need to manage passkeys at scale and provide users with a consistent experience across devices.

The solution is designed to enable an organization to increase security without adding to the burden on the end user, Caimi said.

This a turning point for the cybersecurity industry, agreed Frazier. "This is one of the first times in my life in security where we've got something that makes things both easier to use and more secure at the same time," he said. "That almost never happens."



Watch the full event here