OUCH! September 2025

Workforce Security and Risk Training

OUCH!

The Monthly Security Awareness Newsletter for You

Passkeys – A Simpler and Safer Way to Sign In

Sarah’s “Strong” Password Wasn’t Enough

Sarah considered herself pretty tech-savvy. She worked in marketing, leveraged numerous online design tools, and protected all her accounts with long, strong passwords. One morning, while checking her text messages over coffee, Sarah noticed an urgent text from her bank: “*We’ve noticed suspicious activity on your account. Click here immediately to login and review your account*.” Concerned, she clicked on the link. The website looked just like her bank’s—same logo, same layout. Everything looked legitimate. Concerned about the security of her account, she typed in her login and password, but the website responded with an error. She tried several more times, but could not login. Just then, she got a pop-up alert reminding her she was late for a team meeting. I can fix this later she thought, as she prepared to jump on the call.

Hours later, her phone buzzed: **$2,000 withdrawn from your bank account.** Her heart sank.

She called her bank immediately. It turned out that the text message was a fake, it was something called a smishing scam. Similar to a phishing email attack, but instead of using email, the attacker used text messaging. The website she visited was also fake, designed to look real and steal her login and password. Even though her password was long and strong, it didn’t matter—**she handed it right over to the cybercriminal.**

The worst part? Because Sarah felt that her password was so strong, she used that same password for some of her other online accounts, something she knew she should not have done. Once the cyber attacker had her bank login and password, they used that same login and password to try logging into her other accounts. Her shopping, streaming, even her email services were suddenly at risk. It was going to be a very long day.

Say Goodbye to Passwords: Say Hello to Passkeys

Are you tired of logging in with passwords, frustrated with having to use different apps and unique codes to prove who you are? Are you concerned that no matter what you do, cyber attackers will find a way to hack into your accounts? Meet **Passkeys**: a simpler, faster, and far more secure way to log into your accounts. What makes Passkeys so exciting is they are incredibly strong and yet much simpler to use than passwords; all you need is yourself to login!

So what exactly is a Passkey?

Passkey is a secret code (technically a cryptographic key pair) created by your computer, with parts of the code stored on both your computer and the website. Your code is unique to that website; every time you set up a new Passkey for another new site, a new, unique code is created and then saved to your computer. When you save your code, you often have the option of saving it to your operating system, password manager, or browser. Once saved, the next time you visit that website, instead of logging in with a login and password, you will most likely be asked to unlock the secret code using something called biometrics. Biometrics are when you use yourself to authenticate, such as your fingerprint or facial recognition. No more passwords to remember or type, no more unique codes texted to you or generated on your phone, just use your finger or face. In addition, your biometric information is never shared with anyone online or any websites, all of your personal information stays local on your device.

Passkeys are relatively new, and every website may implement them in a slightly different way. In some cases, you may be asked to still login with your password, then confirm who you are with your Passkey. If you are asked to still use passwords, as always make sure every password is unique and strong. When you use a Passkey to secure your account, not only are you simplifying your life, you are helping lock out some of the most advanced cyber attackers from around the world.

Guest Editor

Dr. Johannes Ullrich is the Dean of Research for the SANS Technology Institute. He founded and currently operates the SANS Internet Storm Center. A SANS Fellow, Dr. Ullrich teaches web application security (SEC522) as well as intrusion detection (SEC503) classes. His daily short-form podcast informs security professionals of the latest cybersecurity news.

Resources

How Cybercriminals Steal Your Passwords: https://www.sans.org/newsletters/ouch/unveiling-shadows-how-cyber-criminals-steal-your-passwords/
How Cybercriminals Exploit Your Emotions: https://www.sans.org/newsletters/ouch/cybercriminals-exploit-your-emotions/
The Power of Password Managers: https://www.sans.org/newsletters/ouch/power-password-managers/
The Power of Passphrases: https://www.sans.org/newsletters/ouch/power-passphrase/