OUCH! December 2025

OUCH!

Workforce Security
and Risk Training

The Monthly Security Awareness Newsletter for You

Overwhelmed by Cybersecurity? Focus on the Core Four

The Story

Maria always tried to stay safe online, but the endless advice left her feeling overwhelmed. She had heard she needed strong passwords, antivirus software, VPNs, firewalls, privacy settings, backups, and more. Unsure where to start, she began by adjusting some of the technical settings on her Wi-Fi router but quickly became confused and eventually gave up.

Later that day, Maria received an urgent text message that looked like it came from her bank. It warned that her account would be locked unless she confirmed her login immediately. Stressed and distracted, she clicked the link and entered her username and password. Within hours, cybercriminals were inside her bank account. Because she reused the same password for some of her other accounts—email, shopping sites, and even social media—they quickly gained access to much of her entire digital life.

Maria didn't fall victim because she didn't care—she fell victim because she didn't know where to start.

The Core Four: Making Security Simple

A major challenge for many people is overcoming this sense of confusion. That's why the National Cybersecurity Alliance (NCA) created the Core Four—a set of four simple yet powerful steps anyone can follow. By focusing on these four actions, you can put your energy where it matters most.

1. Strong, Unique Passwords (and a Password Manager)

Your passwords are the keys to your digital life. Unfortunately, cybercriminals are constantly trying to steal or guess them. If you reuse the same password across multiple accounts, one stolen password could unlock everything.

Here's how the Core Four approach simplifies this:

- Use **long and unique passwords** for each of your accounts. One easy method is to use a passphrase, a string of multiple words that's easy to remember but hard to guess. In some cases, you may be also asked to include a mix of letters, numbers, and special characters.
- Don't try to remember all your passwords —let a **password manager** do the work for you. These tools generate strong passwords, store them securely, and fill them in automatically when you log in to your accounts. Think of a password manager as your personal security vault. Once you set a strong master password, it handles the rest, reducing stress and saving you time.

2. Multi-Factor Authentication (MFA)

Even the strongest password isn't perfect. That's where multi-factor authentication (MFA) comes in. Also known as two-factor authentication or two-step verification, MFA adds an extra layer of security by requiring something in addition to your password—such as a code sent to your phone, a fingerprint, or a security key.

Why does this matter? If a cybercriminal steals your password, they still can't access your account without the second factor. Turn on MFA wherever possible, especially for your most important accounts.

3. Automatic Updates

Cybercriminals are always looking for weaknesses in software and apps. When companies discover these flaws, they release updates to fix them. If you delay installing updates, you leave the door open for attackers to exploit known vulnerabilities. The easiest solution is to enable automatic updating on your devices, apps, and accounts. This ensures security fixes are applied in the background, often without you lifting a finger.

4. Spot and Stop Social Engineering (Scam) Attacks

Cybercriminals don't always need technical tricks—they often rely on manipulating people. This tactic is called social engineering, and it includes like phishing emails, fake text messages, and phone calls designed to trick you into clicking links, downloading malware, or sharing your credit card information or password.

Here are some red flags to watch for:

- **Urgency:** "Act now or lose access!"
- **Too good to be true:** "You've won a prize!"
- **Requests for sensitive information:** passwords, PINs, or bank details

When in doubt: stop, slow down, and verify.

Staying Safe Made Simple

Security doesn't have to be complicated. By focusing on the Core Four, you can build online habits that actually stick. Whether it's your coworkers, kids, parents, or community, the Core Four offers a simple yet powerful way to help everyone stay safer online.

Guest Editor

Jennifer Cook is the Senior Director of Marketing at the National Cybersecurity Alliance. She leads the organization's marketing strategy and oversees campaigns that engage millions of people. Since joining in 2017, Jennifer has spearheaded initiatives including Cybersecurity Awareness Month and Data Privacy Week, collaborating with partners worldwide. https://www.linkedin.com/in/jennifer-h-cook/

Resources

National Cybersecurity Alliance: https://staysafeonline.org
The Power of Updating: https://www.sans.org/newsletters/ouch/power-updating/
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/

You can find more Ouch! On the following link: https://www.sans.org/newsletters/ouch