PUBLICATION

Cybersecurity Awareness Month 2025: Seven Foundational Pillars of Good Personal Cyber Hygiene

Authors: Justin S. Daniels
October 09, 2025

Deepfakes, social engineering, and urgent texts or calls from your IT department all continue to be effective methods hackers use to gain access to your most important accounts and assets. October is Cybersecurity Awareness Month, and just like washing your hands, good cyber hygiene protects you from problems that can evaporate years of work to create financial security for you and your family. The stakes are as high as ever, as poor cyber practices can lead to stolen identities, financial loss, reputational damage, or even the downfall of a business.

Here are the seven foundational elements of your digital defenses:

1. Use a Password Manager – Your Digital Keychain

The average person has about 66 online accounts. Remembering dozens of complex passwords is impossible. That's where a password manager comes in. Think of it as a locked safe that stores all your digital keys.

- **Why it matters**: If you reuse passwords or rely on memory, you're one phishing email away from losing control of multiple accounts.
- **How to do it**: Choose a reputable password manager and use it consistently. Store your logins there.
- **Pro tip**: Protect the vault with a long, memorable master phrase (see Tip #2).

2. Create a Long Master Passphrase – and Add a Twist

The trick to making your password strategy resilient is layering.

- Start with a **long, memorable phrase** as your master password. Example: *Running$makesmehappy5%*.
- Then, add a **personal, secret word at the end** of every password that only you know. Example: *shoes*.
- **Why**: Even if a hacker breaks into your password manager, they won't have your private add-on word. That additional layer can be the difference between a compromised account and a blocked attack.

3. Enable Multifactor Authentication (MFA)

A password alone is like locking your front door while leaving the key under the mat. Multifactor authentication (MFA) adds a deadbolt.

- **What it looks like**: A code texted to your phone, a mobile authenticator app, or a hardware key.
- **Why it's critical**: Even if an attacker steals your password, MFA adds an extra hurdle that acts as an additional layer of defense.
- **Where to use it**: Always enable MFA on email, banking, and cloud storage accounts. Use it to protect your most sensitive accounts.

4. Watch Out for Phishing – Think Before You Click

Phishing emails – and now texts – remain the number one way attackers access your accounts. They prey on urgency and fear.

- **Red flags**: Messages claiming "your account will be locked," requests to "verify your identity," or too-good-to-be-true offers.
- **Good habit**: Hover over links before clicking. If you weren't expecting an attachment, don't open it.
- **Golden rule**: Assume any email or text you did not expect is false until proven otherwise. If something feels off, trust your gut and verify with the sender through another channel (call, text, or a fresh email – not "reply all").

5. Never Trust Urgent Bank or Exchange Requests

If you receive an email or phone call claiming to be from your bank, cryptocurrency exchange, or payment app demanding you "act immediately" to change your password or share personal details, assume it's fake.

- **Why attackers do this**: They exploit fear and urgency to make you act without thinking.
- **What to do**: Hang up or delete the message. Then, contact the bank or platform using the official number on their website or app.
- **Bottom line**: Legitimate institutions will never pressure you to reveal sensitive information over email or a call.

6. Verify IT Department Calls

Attackers know employees trust IT. That's why "tech support" scams are so effective. If someone calls claiming to be from your IT department with an urgent request – reset your password, install software, share a code – hang up.

- **Good practice**: Call your IT team back using the official helpdesk number or ticketing system.
- **Why it matters**: A quick verification call can stop attackers from gaining access to your network with your help.

7. Keep Devices and Software Updated

Think of updates like the flu shot for your digital life. Hackers constantly look for "holes" in old versions of software. Updates patch those holes.

- **Automatic is best**: Set operating systems, browsers, and apps to update automatically.
- **Do not delay**: Hitting "remind me later" is like ignoring the smoke alarm battery. It may work fine today, but it leaves you vulnerable tomorrow.
- **Scope**: Update everything – phones, laptops, routers, and even smart devices like thermostats or cameras.

Final Word

Practicing good cyber hygiene isn't about becoming a cybersecurity expert – it's about building consistent habits and accepting a certain level of inconvenience for security's sake. Use a password manager. Strengthen your passwords with a personal twist. Lock down your accounts with MFA. Think before you click. Don't fall for urgent scam requests. Stay updated.

The SEC, FTC, and regulators worldwide are watching how companies protect data. But the truth is, cybersecurity starts with each of us. The strongest firewalls and policies won't matter if we emulate President Skroob from *Spaceballs* and use the password "12345." Think of these seven pillars as the foundation of a much more secure digital life.

For more information on personal cyber risk, contact Justin Daniels or any member of Baker Donelson's Data Protection, Privacy and Cybersecurity Team.

October is National Cybersecurity Awareness Month

Observed annually in October, Cybersecurity Awareness Month is a collaborative effort between the public and private sectors to raise awareness about cybersecurity. It was launched in 2004 by the U.S. Department of Homeland Security (DHS) and the National Cyber Security Alliance (NCSA).

Throughout Cybersecurity Awareness Month, we will provide proactive tips and information in order to mitigate your cyber risks.