GREATEST HITS

Cybersecurity Awareness Month 2024

A conglomeration of the best tips from CISA, NCA & Expel

Each year during Cybersecurity Awareness Month, the Cybersecurity and Infrastructure Security Agency (CISA) and the National Cybersecurity Alliance (NCA) provide resources to raise awareness and help secure the digital world.

Expel is celebrating the month with our own theme: a secure world is built together. Security is a team sport, and we're doing our part with this list: we've compiled a ton of great tips into one resource and download. This list isn't exhaustive, but we've gathered some key points to remember for the month year.

TIPS FOR BUSINESSES

These are tips for security practitioners and business leaders to keep in mind when securing and building their environments.

✓ Keep your teams updated about updates.

Sharing regular updates on system and tool availability, known vulnerabilities in previous versions, and setting deadlines for updates helps keep your teams more secure. Bonus: enabling auto-updates simplifies the process even further! Learn more.

✓ Keep up-to-date with Patch Tuesday.

On the second Tuesday of every month, CISA releases a list of the latest known vulnerabilities wreaking havoc. Expel posts a condensed version of that list with remediation actions—you can find them on our blog. Learn more.

✓ Frameworks are your friend.

Popular cybersecurity frameworks—like NIST CSF—can provide guidance on how to get started and keep up with cybersecurity strategic planning. Use these free tools to get (and stay) secure. Learn more.

✓ Mergers and acquisitons (M&A) are security events and should be treated as such.

We've all heard stories about M&A events that resulted in security nightmares, from unexpected new endpoints to clashing technologies. Keep your security teams updated on these activities so they can plan and prepare to merge tech stacks accordingly! Learn more.

✓ Save money by investing in quality security training programs.

Good employee training can save money and prevent breaches, and using AI to detect threats earlier and faster can reduce costs too. (Gamification, anyone?) Learn more.

✓ Employees who work from home are part of your threat landscape.

Don't forget to consider mobile devices and home networks when creating and designing your security policies. Be sure to provide clear guidelines, and remind your teams that their home network is an equal opportunity for bad actors to exploit. Learn more.

✓ Mobile devices are breachable—don't forget to teach your teams how to secure them.

Provide education on shadow IT—apps and software used on a device the owner (or security teams) might not know about. Use least-privilege rules for mobile devices (and in general). Learn more.

TIPS FOR EVERYONE

Whether you’re applying them to your personal or professional life, these are beneficial to keep in mind or action to keep yourself and your business safe.

✓ Don’t just learn to recognize phishing–report it.

Whether it’s to your IT team, Gmail, or a governing agency, let someone know when it happens. Look for: urgent or emotional language, requests for personal information, untrusted URLs, or incorrect links or email addresses. Learn more.

✓ Strong passwords are forever, because it’s that helpful.

Creating and (safely) storing strong passwords is one of the easiest ways to protect yourself. Use a trustworthy password manager (not that sticky note under your keyboard), and make passwords complex and long. Learn more.

✓ Enable multi-factor authentication whenever possible.

It’s as easy as flipping a virtual switch in your settings for any app that offers it. Whether it’s at work or for personal accounts, turn it on! Learn more.

✓ Teach kids how to navigate the online world safely.

Kids are an easy target for bad actors, especially since they don’t immediately assume bad intent. Educate your kids on suspicious online activity, so they know when and how to let you know!

✓ Delete apps you no longer use.

Apps store data, and even if you don’t use it, it may still be running in the background on your device. Fully log out of and delete old apps (and accounts) when you no longer use them.

✓ Keep an eye out for newer scams, like pig butchering, so you can learn the signs.

Ever get a random text from a number you don’t know? It could be a pig butchering scam, where the bad actor wants to “fatten up” your investment (emotionally and financially). Don’t respond at all—even to say “wrong number”—to these texts. Learn more.

✓ Freeze your credit (everywhere) by default without impacting your credit score.

It’s free to do, and you can quickly unfreeze it when you apply for loans, credit cards, and so on. Contact each of the three credit bureaus, and keep it frozen. Read your reports regularly and dispute anomalies immediately! Learn more.

Bonus tip: freeze your kids’ credit too, as they’re often a target since it’s more likely to go unnoticed.

✓ Watch for deceptive design tactics.

Deceptive design happens when businesses–especially e-commerce–make it hard to unsubscribe or cancel. Be sure to read the fine print, be careful with the personal info you share, and if it’s too good to be true, than it is.

More security questions? Reach out to an Expel expert, or visit our Cybersecurity Awareness Month resource center for more information. Learn more.

MORE SECURITY QUESTIONS?

Reach out to an Expel expert, or visit our Cybersecurity Awareness Month resource center for more information.