TIPS FROM THE SOC

expel

How *everyone* can enhance cybersecurity resilience

Lessons learned from Q3's Quarterly Threat Report

To help strengthen security for everyone, we're sharing key lessons from our SOC's findings, along with practical tips for staying safe—whether you're a security expert or not—this month and beyond.

The latest resilience tips from Expel's SOC

To protect against fake error messages & captchas

□ Restrict the ability to run processes with administrative permissions to only users who need 4it, and grant those privileges temporarily only when needed.

□ Deploy endpoint detection and response tools—on endpoints and servers—to protect assets and prevent attacks.

□ Limit PowerShell access for standard users as much as possible. You can use tools like Windows Defender Application Control (WDAC) and AppLocker.

□ Require PowerShell to operate in Constrained Language mode to limit the capabilities of common cmdlets that are often used to download a bad actor's main payload.

□ Enable PowerShell script block logging to allow any suspicious activity to be reviewed.

To protect against high-risk malware like Lumma

□ Prepare a playbook for steps to take if an infostealer malware is executed in your system. Be sure to include instructions for how to remediate cloud infrastructure credentials that may be stored on a device.

□ Implement a password manager. Even if malware is deployed, your credentials will remain encrypted and safe from bad actors. And don't forget to give contractors access, too!

To protect against phishing-as-a-service (PhaaS) platforms

□ PhaaS platforms often target business email compromise (BEC)—monitor and investigate logins from hosting providers. Tools like Expel Workbench™ or APIs like ipinfo.io, AbuseIPdb, Spur, can help identify the type of login.

□ Track information about incidents over time. Tracking patterns can help identify malicious hosting providers, allowing your team to spot and identify incidents more quickly.

To protect the software supply chain

□ Maintain a software bill of materials (SBOM) with guidance from the USA's National Telecommunications and Information Administration's guidelines.

□ Use automated tools to continually assess your risk level associated with software dependencies.

□ Prevent typosquatting by using commit hashes for your GitHub Actions in your yml files, instead of using the exact name of the Commit to prevent usage of a malicious repository.

Tips for non-technical cybersecurity stewards

How to help support your security team

□ If it looks suspicious, call it out. This is the easiest way to keep you and your organization safe. This includes your personal time online, too!

□ Don't just delete phishing emails–report them. They help your security team learn how to protect your org faster next time, so follow the correct steps to report suspicious emails.

□ Use the password manager recommended to you by your security team. These aren't optional, and choosing not to use them makes you a bigger risk for your organization.

□ If you're being asked to copy and paste a fix or an update, stop what you're doing and confirm it's legitimate before taking action. It's better to be safe than sorry.

□ Stay vigilant and patient. And if you do make a mistake—or even if you aren't sure—let the right team know ASAP. Your security team is there to help you!

□ Complete your security training. Most expire and require action at least once a year to remain compliant. You don't want to be the one person putting your entire business at risk.

Read the full report on our blog →