VISIT OUR FRAUD HUB

8 ways to stay cyber smart

Use these tips to help you protect your data and financial information.

Cybersecurity is a critical business function. It should be just as important as sales, human resources and business operations.

By being proactive and vigilant, you can help protect your organization's data, finances and business processes. Use these eight tips to build an incident response plan or review and fortify your cybersecurity defense strategy.

1 Have a plan

Outline the steps you'll need to take to prevent an attack—and what you'll do if you are targeted. Your plan should cover protection, identification, detection, response and recovery. Planning shouldn't fall only on your chief information security officer or technology teams. Create holistic teams across your organization that can plan for various risks and act quickly if a cyber event occurs. A sound plan can help your business function for up to two weeks without access to certain systems.

2 Test, test, test

You'll never know how good your plan is if you don't test it. Does your plan consider all possible attack vectors? Does everyone know what to do when something goes wrong? What if communications are offline or compromised? Who is responsible for activating your incident response plan? Test your plan regularly and fix any gaps that emerge.

continued on next page >

VISIT OUR FRAUD HUB

Educate everyone

Your entire company should complete regular cybersecurity training—from interns and contractors to employees, including executive leadership. Training can include educational videos, webinars and other interactive tools. Refresh the training with evolving attack scenarios, such as social engineering, credential stuffing tactics and mobile device compromise. Physical security is also important. The person walking through the office with an official-looking polo shirt might not be an approved vendor or invited guest.

Phish for answers

Business email compromise (BEC) is one of the leading ways that cybercriminals can infiltrate a company and trick employees into divulging confidential information or sending fraudulent payments. Create a phishing awareness and testing program to check your employees' email security protocols. Conducting regular phishing and social engineering tests can help reduce the chances of an attack.

Don't sit still

Cybercriminals are always changing their methods and evolving with technology. You should too. Stay up to date on ransomware information so you can implement effective countermeasures. Consult resources like the U.S. Cybersecurity & Infrastructure Security Agency (CISA) and sector-specific Information Sharing and Analysis Centers (ISACs) that spread critical security information across industries.

Divide to conquer

Use network segmentation to isolate parts of your network so that if attacked, only a small portion of your network is affected. You can implement the same concept with data storage, access management and physical access controls. Consider adding an application "allow list" that only permits certain apps on your network. Create multiple networks to lock sensitive systems and data. No users should be trusted by default, and everyone should be verified and authenticated before accessing your network.

Layer on the protection

Think about security in terms of rings, with the most precious assets in the center. At the outermost layer, you should start with domain security to prevent spoofing and domain takeover. Consider deploying a web application firewall to inspect internet traffic as it comes into your company. The protections continue as you progress to the system's core and your data—which should be encrypted. This layered protection applies to hardware too. You should also require multifactor authentication—such as a one-time password or token—in case a username-password combination is compromised.

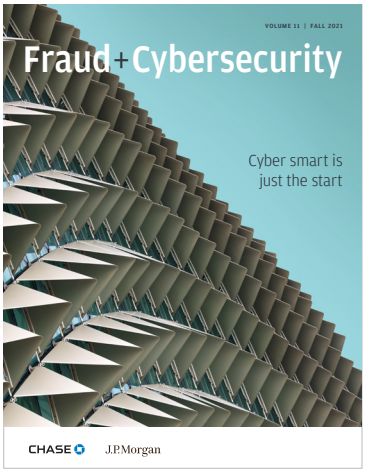
Create a virtual cyber council

Establish relationships with experts in multiple cybersecurity agencies to be your go-to resources for advice and strategic guidance. For instance, you could add law enforcement and the FBI to your council. If you have cloud operations, find someone who can guide your decisions around tools, policies and operational risk. Industry regulators are also great resources. Recognizing you don't have to know it all is an asset, not a liability. Using experts where needed can bolster your cybersecurity program.

Key takeaway

- Visit our Cybersecurity and Fraud Protection Insights page to learn more about how JPMorgan Chase experts can help keep your organization safe.

The previous article is an excerpt from Fraud + Cybersecurity Magazine: Fall 2021.



DOWNLOAD