



Cybersecurity in the Hacking Age: Best Practices for Prevention and Detection



Two hours. That's all it takes for a hacker to get to the data they need once they gain entry to an organization's computer systems. Most companies are not

prepared to address a breach that quickly. In fact, many don't even realize they've been breached until it's too late to recover lost funds or data without repercussions.

KeyBank recently examined how hackers operate today and how businesses can defend themselves. We joined forces with the experts at Binary Defense™, a leading cybersecurity solutions provider that focuses on helping businesses identify threats earlier, and TrustedSec, an information security consulting team at the forefront of attack simulations.

"Technology is moving so fast and furious we have to think differently about how we do things personally and how we do things at work," says Tammy Gedetsis, Senior Information Security Consultant at KeyBank. Gedetsis is responsible for cybersecurity education and awareness programs for Key employees and the bank's clients, both businesses and individuals.

One thing is clear: with cyberattacks becoming faster and more sophisticated, education about prevention is necessary for everyone.

How attacks are conducted: Hackers as social engineers

The first step to protecting yourself and your money is understanding how hackers think and act. The stereotype of a hacker as a loner in a basement writing code is outdated. Today's hackers are using "social engineering" to take information they glean from social media and publicly available information, such as speaking engagements and media profiles. Armed with that data, they target people using personal details that make them feel comfortable sharing pertinent information.

Hackers can spoof phone numbers or email addresses to look like they're coming from within the company or from a legitimate financial or mobile service provider. They ask questions or send links that mine for personal data, such as credit card numbers and identifying information. Once one person within an organization has been compromised, hackers may gain the access they need to take down the whole system—quickly.

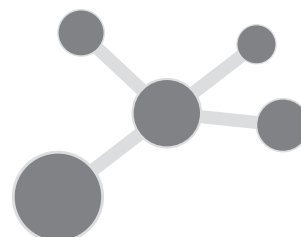
In addition, breaches are not just happening online; cybercrime can originate in the non-digital world. Some hackers operate "physical penetration" schemes to gain access to secure systems. They use tactics such as operating in pairs, creating diversions and impersonating employees or visitors, and tools such as badge cloners and under-door opening tools to get into buildings and onto employee computers, sometimes even machines located in locked and secure areas.

Some Common Attacks	Description
Credential Stuffing	People who use the same password across multiple systems are particularly at risk for having their password compromised on a more vulnerable site and then used to gain access to financial or employer sites in a mass password test.
Business Email Compromises	Hackers impersonate executives, employees, or trusted vendors and infiltrate legitimate email threads, then use access for fraudulent deals or to redirect funds or wire transfers.
Ransomware	Hackers gain access to systems via an external link that an employee clicks on, typically through a phishing attack. They then encrypt large amounts of critical data, which an organization must pay a large ransom (that can be six or seven figures) to release.
Data Theft	Hackers are focused on gaining access to a corporation's research and development files and intellectual property (IP), often committed on behalf of foreign nations or corporations.

Who are the hackers?

Cyberattacks are well-researched and well-coordinated, and unfortunately the perpetrators are very rarely caught or punished. Hackers are often part of a large network of organized crime or, less commonly, are state-sponsored actors. Organized crime can be focused on gathering Personal Identifying Information (PII) or Personal Health Information (PHI), which are sold on the black market for identity theft; stealing and selling Internet Protocol (IP); selling compromised accounts; and committing ransomware attacks. State-sponsored actors, including those from Russia, China, Iran, and other countries, may be gathering business or state intelligence or IP that could support the government or be used in military preparedness.

General hacking includes individuals who sell solutions such as customized malware or compromised accounts. These independent hackers are commonly hired for personal actions, such as allowing a person to spy on their mate by gaining access to their email accounts.



Hackers are often part of a large network of organized crime or, less commonly, are state-sponsored actors.

Protect yourself or your business from cyberattacks

Once you understand the nature of cybercrime, it's time to get smart about avoiding it. While nothing is foolproof, there are tangible steps you can take to ensure you are not an easy target for hackers. Keeping your personal or business information safe from breaches is possible with some easy-to-employ, but often-overlooked, measures.

Top Five Ways to Keep Your Information and Systems Secure

1. Use two-factor authentication everywhere you can.

Yes, it can make logging in more time-consuming, but it's much more difficult for a hacker to breach your password and access your PC or phone.

2. Make your passwords more complicated and use different ones for different sites or a password vault. Use phrases that are longer, rather than generic word and number combinations that fall into a pattern (e.g., Fall2019, Winter2019). A phrase such as ILoveBuckeyes! is more difficult to hack. If remembering multiple passwords is an issue, try a recommended password vault provider, an online service designed to help keep your password information secure and consolidated into one location, such as 1Password, KeePass, LastPass, or Dashlane.

3. Make sure you keep your computer software

up to date. Security updates are designed to fix known attacks or vulnerabilities that software developers are monitoring and addressing.

4. Be careful of how much information you share on social media. Social engineers can track your spending habits, location, busy times on your schedule, travel plans, and more and strike when you're preoccupied, attending functions, at work, or traveling. That catchy Facebook quiz? Watch out if it asks for too much personal data like your birthdate or address.

5. Do not give out personal information without verification. Hackers can impersonate financial services providers. If you receive an email or phone call that looks official, do not respond directly. Use the phone number on your financial services provider's statements to call and confirm whether the call/email was genuine. Never give out your Social Security number or credit card information to an unverified person on the phone, and avoid clicking on any links in emails you receive.

KeyBank is your partner in secure systems

According to the Association for Financial Professionals 2019 Fraud and Control survey, 82% of respondents said they were targets of payments fraud in 2018. With the number of actors involved and the complexity and speed of attacks increasing, educating your employees about prevention and detection is critical. KeyBank is committed to helping you protect your business and your treasury management system from fraud interference.

To learn more about how Key can help support your company's information security efforts, **visit key.com/security or contact your KeyBank Payments Advisor.**



Cybersecurity in the Hacking Age: Best Practices for Prevention and Detection

3 of 3