5 Common Cybersecurity Mistakes and How to Avoid Them

All organizations, regardless of their size or industry, are at risk of being targeted by cybercriminals. These malicious actors can conduct cyberattacks, leading to significant financial, operational and reputational damage that can be difficult or impossible to recover from. Fortunately, solid cyber hygiene practices can reduce the likelihood of data breaches and other cyber incidents from occurring, and many of these practices are relatively low-cost and easy to implement.

This article explains five common cybersecurity mistakes organizations make and provides actionable solutions for each.

1. Weak or Reused Passwords

The Mistake: Users often resort to simple passwords they can easily remember. They also may use the same password for multiple devices and accounts.

Why It Matters: Cybercriminals can more readily exploit weak, easy-to-guess passwords to gain unauthorized access to devices, networks and accounts. Using weak passwords increases data vulnerability, and reusing passwords across different systems can compromise multiple accounts from a single breach.

How to Avoid It: To address these issues, employers should require that staff use unique and strong passwords for each account, device and network. They should also mandate that these login credentials be changed regularly. Passwords should not be common or predictable (e.g., “password”) or sequential numbers or letters (e.g., “12345” or “abcde”). Using a combination of upper and lowercase letters and special characters can strengthen passwords. Employees can also consider using a verified password manager to store and generate passwords securely.

2. Ignoring Software Updates

The Mistake: Software and system updates are delayed or neglected.

Why It Matters: These vital updates often contain patches that address known vulnerabilities. When they are not installed, attackers can exploit outdated software or known security gaps to gain access to or control of devices, networks or systems.

How to Avoid It: Cybersecurity policies should require that automatic updates are enabled on all devices and applications. There should be processes that regularly check for and install updates, especially for security software that protects against viruses, intrusions and other threats. Employers should also stay informed about critical updates released by software vendors so they can be implemented without delay.

3. Lack of Employee Training

The Mistake: Employers may fail to educate employees about cybersecurity best practices.

Why It Matters: Human error is a leading cause of security breaches, and employees who are unaware of common schemes cybercriminals use (e.g., social engineering tactics in which the target is tricked into revealing their password or other sensitive information) may more easily fall victim to them. Untrained employees may also be unaware of safe data handling best practices and can inadvertently compromise security.

How to Avoid It: Employers can implement cybersecurity training sessions for all employees upon hire and at regular intervals. To increase engagement and enhance learning, training should include interactive modules and real-life scenarios. These sessions should also provide an opportunity for employees to raise questions or concerns and encourage a culture of cybersecurity awareness within the organization.

4. Overlooking Multifactor Authentication (MFA)

The Mistake: Users may rely solely on one password for account and device security.

Why It Matters: Cybercriminals can steal or guess passwords, especially if they are weak. MFA adds an extra verification step and significantly reduces the risk of unauthorized access.

How to Avoid It: Employers should require MFA on all business accounts and devices that offer it, especially those containing sensitive information. This process requires users to verify their identity through a separate form of

authentication (e.g., a time-based one-time password sent through text message or email). Employees should use authentication apps or hardware tokens for secure verification and regularly review and update MFA settings to ensure optimal protection.

5. Using Unsecured Public Wi-Fi

The Mistake: Sensitive information is often accessed over publicly available Wi-Fi networks without password protection.

Why It Matters: Publicly available Wi-Fi can be a hot spot and entry point for cybercriminals to access networks and intercept data. Unsecured networks increase the risk of man-in-the-middle attacks, in which a malicious actor intercepts communications between two parties, reads the information, potentially alters it and transmits the communication without either party recognizing this is occurring.

How to Avoid It: Employees should avoid accessing sensitive information on public Wi-Fi and only use trusted networks. They should also turn off automatic Wi-Fi connection and file-sharing settings to prevent unintended connections or data leaks. Additionally, employees should ensure they use virtual private networks, or VPNs, that encrypt data transmissions if they are connecting to public Wi-Fi and confirm their firewall is enabled to add protection against malware and other cyberthreats.

Conclusion

Cyberattacks are a serious threat to all organizations, and cybercriminals often exploit vulnerabilities created by poor cyber hygiene practices. By recognizing these mistakes, realizing their significance, taking action to avoid them and implementing cybersecurity best practices, organizations can improve their cybersecurity posture and reduce the risk of costly cyberattacks occurring.