TRUSTEDSEC

Preventing Cybercrime:
How to Protect Yourself From Cybercriminals and Identity Thieves

What is the Threat?

In today's digital landscape, cybercrime is more prevalent than ever. High-profile incidents, such as the 2023 ransomware attacks on Caesar's Palace and MGM, underscore the devastating consequences of data breaches. Caesar's Palace paid $15 million to hackers, while MGM ultimately faced losses in revenue exceeding $110 million. The personal information of thousands of customers and employees was exposed. Incidents like this serve as a reminder that no one is immune to the dangers of cybercrime.

Why are Cybercriminals Still Successful?

It often comes down to two major vulnerabilities:

1. **Technical Flaws:** Weaknesses in the programs and misconfigurations in the technology we use every day can open the door for hackers.
2. **Human Flaws:** Social engineering, where cybercriminals exploit human behavior, is responsible for up to 90% of all malicious breaches.

While you may think that cybersecurity requires advanced technical skills, the truth is, you are your own best defense. Cybersecurity starts with building simple, sound security habits into your daily routine. By recognizing that you're a target, you can better protect yourself and your organization.

What Do Cybercriminals Want?

Cybercriminals aim to steal:

- Personal financial and healthcare information
- Company secrets or proprietary data
- Login credentials for financial accounts, social media, or corporate systems

What's Your Role?

Everyone has a part to play in cybersecurity. Whether you're an individual or part of an organization, understanding your role in protecting data is crucial. You don't have to be a tech expert, but you do need to be aware of the risks and take proactive steps to safeguard information.

Questions to Consider:

- **What do cybercriminals want, and how do they try to get it?**
- **How can I contribute to the security of my organization's data?**

What Is Sensitive Information?

Cybercriminals target individuals and organizations of all sizes. You don't have to be a high-profile CEO to become a victim. In fact, small businesses are often more vulnerable because they have fewer resources dedicated to cybersecurity.

Sensitive Information Includes:

- Personal data (name, address, Social Security number)
- Financial information (credit card details, bank account numbers)
- Healthcare data (patient IDs, diagnosis information)
- Corporate data (trade secrets, client information)
- Login credentials (passwords, PINs)

Who Are Cybercriminals?

Forget the stereotype of hackers as hooded figures hiding in dark rooms. In reality, cybercriminals can be anyone:

- Former employees seeking revenge
- Foreign agents looking to disrupt or steal data
- High school or college students experimenting with hacking tools
- Well-organized and financed criminal organizations

Top Tips for Protecting Yourself:

1. **Use Strong Passwords:** Create unique, complex passwords for every account. Reusing passwords is a common way that accounts are compromised. Consider using a password manager to maintain multiple strong passwords conveniently and securely.
2. **Enable Multi-Factor Authentication (MFA):** Add an extra layer of security by enabling MFA on your accounts. This requires a second form of identification, such as a code sent to your phone or an authentication app on your phone. While using a code texted to your phone may be more convenient, authentication apps are generally more secure.
3. **Be Wary of Phishing Scams:** Don't click on suspicious links or download attachments from unknown sources. Always verify the legitimacy of emails or messages. When in doubt, call your bank or the organization that the email or message claims to be from to verify.
4. **Update Software Regularly:** Keep your software, apps, and devices updated to patch known vulnerabilities.
5. **Monitor Your Accounts:** Regularly check your financial statements and online accounts for any unusual activity.
6. **Back Up Your Data:** Regularly back up your files to an external drive or secure cloud service in case of a ransomware attack or other cyber incident.
7. **Be Wary:** Scammers will often pretend to be from a trusted organization. If something seems off, it probably is. Advances in AI voice spoofing are making these types of attacks more effective and more difficult to spot every day.

By adopting these simple security measures, you can make yourself a harder target for cybercriminals and help protect your organization from costly data breaches.