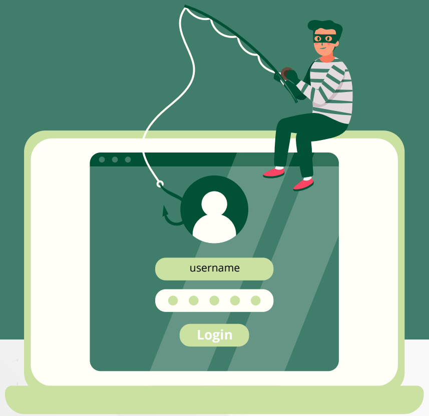
TOP 3 Business Cyberattacks And How to Prevent Them

Education is the first line of defense in protecting your business against cybercriminals. Learn about the three most common types of attacks businesses experience so you can take steps to prevent them.



1. **Social Engineering/Phishing Attacks:** This type of attack often arrives in the form of a deceptive email. Criminals pose as a legitimate company, employee, or outside vendor in order to trick the recipient into clicking on a malicious link, opening an attachment, or responding with sensitive information.

   - **What You Can Do:** Train your employees to recognize the features of phishing emails. Many organizations send out test emails to assess employees' skills at recognizing and avoiding suspicious messages. If too many people are clicking on and opening things they shouldn't be, additional training may be needed.

2. **Ransomware:** This is a type of malware (usually contracted through phishing emails or web downloads) in which attackers take control of your systems and data and demand payment to unlock everything. The FBI generally recommends against paying a ransom, but some organizations decide it will be less expensive to pay the ransom than to spend time and money on recovery. However, there is no guarantee that everything will be restored after the ransom is paid.

   - **What You Can Do:** Conduct regular backups of your computer files. In the event of a ransomware attack, you will be able to regain access to everything from the backup instead of paying the fee. Employee training, as mentioned above, will also help protect your company against ransomware attacks.

3. **Advanced Persistent Threats (APTs):** This is an attack on the integrity of your company's data, whether internal information or customer data. APT attackers are not trying to disable your network; rather, they gain access and go undetected as they steal sensitive information. This is what we see in most high-profile security breaches - criminals are after customer information such as credit card numbers and anything else they can use or sell on the dark web.

   - **What You Can Do:** In addition to employee training, make sure your computer software is up to date, use a firewall and malware filters for email and web browsing, antivirus software, and other forms of defense.