5 Common types of **Security Breaches** in the industry.

The Internet can be a very dangerous place because there are some tech-savvy individuals that engage in various types of criminal activities Online or by abusing computer networks. By exercising vigilance and following security best practices, users can be protected against Phishing, Ransomware, Malware, Identity Theft, Cyber Scams, and some of the other most common types of Cyber Crimes in the industry.

Phishing

Criminals attempt to trick unsuspecting users into doing something they wouldn't ordinarily do, such as clicking on a malicious URL (Link) or email attachment.

Protection Tip: Exercise caution and **DO NOT CLICK** on suspicious links or email attachments. look out for tell-tale signs like frequent grammar or spelling mistakes on "official" correspondence.

Ransomware

This type of breach mostly affects businesses that need access to sensitive data in a timely manner. Data on a victim's computer is locked and payment is demanded before access is returned.

Protection Tip: In addition to following the anti-phishing steps, users should formulate a data recovery plan for their computers. **BACK UP DATA** on a regular basis!

Malware

Any piece of software that was written with the intent of doing harm to data, devices or to people. Viruses, Worms, Trojan Horses, Spyware, Adware are common forms of malware.

Protection Tip: Check the Web Domain! The website might be a fake and could attempt to steal users' login information and personal credentials.

Identity Theft

Attackers can conduct countless criminal activities with a person's identity. They can seize control of a victims' banking credentials, apply for new banking accounts, commit insurance fraud etc..

Protection Tip: DO NOT reveal too much personal information Online and protect your Identity Number at all cost.

Cyber Scams

In many cases, they convey an enticing offer that attempts to trick users into sending money or divulging personal information to the fraudsters.

Protection Tip: When something sounds **TOO GOOD TO BE TRUE**, it probably is. Never buy into incredible scenarios where you are offered money or other rewards in exchange for a fee.