What are some of the cyber criminal tactics used to expose your business?

Email Phishing - This is a technique used by criminals to gather personal information. Phishers send authentic

Spear Phishing - In this more sophisticated technique, the criminal uses personal information often obtained from social media sites helping them pose as a colleague or other close business source to make it appear more valid. Read more

Key Logger - A phishing email can include a link that has no apparent harm but silently downloads a key logger that matches up links you click with login information. This provides the hackers with the website, user ID and password. Since many people use the same credentials for several sites, the criminals then try them on the most common websites that people have accounts on.

Email Spoofing - This is an email that appears to be from a legitimate sender rather than the real criminal sender. Usually, the email address will be very close to the legitimate one. The unaware recipient proceeds to click on a link in the email or reply, providing the criminal with sensitive information or potentially access to your system.

Lost Email Credentials - Cyber criminals often deceive an employee into providing credentials. For example, they may send an email stating someone they know shared a file and include a link to a fake page that resembles Office 365 and request employee credentials or the criminal sends an email appearing to be from Google stating their account has been compromised and need to change password. Again including a link to a website that resembles google log in page where the employee enters their credentials.

Malware Attack - This is when a malicious file or a link is sent to an innocent employee who opens it. It could be sent through email, in a shared file, as a zoom link, or delivered as an attachment using MS Teams, etc. 92% of malware is sent via email.

Ransomware Attack - This form of malware encrypts a business's files which are then held ransom until the business pays the criminal to restore access to the data files. Paying the ransom does not guarantee you will get your files back. This is why having a good backup is crucial as you can restore yourself back to a prior state to the attack ensuring the ransomware is not on your machines. Paying the ransom may get you a decryption key, and you can access your files again, but the virus is still on your system just ready to be triggered again.

Email phishing attempts and malware attacks have increased during the COVID-19 pandemic. Cyber criminals are using the pandemic to exploit and target devices, networks, and personal devices.

Google indicated they stopped 18 million malicious emails each day during just a week in April alone in addition to 240 million spam messages related to COVID-19.