Haekka

Lesson 1 | Security is Everybody’s Job

Updated 2020-09-14

The most secure data is data that is locked up and inaccessible. This is not a reality today as systems, networks, individuals, phones, home devices, and clouds are connected to one another 24/7. Additionally, data drives many technologies and services today, meaning data has to flow within and between corporate systems. This new world of interconnected systems and data as a valuable asset changes the strategy and operations of security.

Security is no longer simply the purview and challenge of the security group. Employees, in all departments of a company, are constantly being targeted by sophisticated, and highly personalized, attacks being managed and run by software systems. These attacks target weak device security, passwords, and human nature.

- There are now databases of billions of real usernames and passwords. These compromised credentials can be used by anybody with a computer willing to buy hacking tools for as low as $20.
- Phishing attacks, with real appearing links, are attempted millions of times per day.
- The average data breach costs close to $4M.

With interconnected systems and software, employees are now the largest threat vector for most companies, meaning employees are the primary target for attackers. Once attackers gain a foothold, even if it is confined to 1 system, they have methods and tools to use that foothold to gain access to systems and data. Often, breaches accounts and systems are not detected for months or even years, meaning attackers have time to gain additional access.

Every employee is a potential entry point into corporate systems for attackers. The best thing you can do is be diligent about the security of your devices and your accounts, both personal and corporate. When it doubt about security best practices or emails with links, be sure to ask questions of your security team before taking any action. It is much cheaper and easier to answer questions before a breach than marshall the resources to investigate and resolve a breach after it happens.

Security is your job. If you have questions or something feels suspicious, ask questions.