Lesson 4 | Threats to You and Your Company

Updated 2020-09-14

The world has changed, as we covered in the last lesson. Shifts in technology and the ways work is done have shifted the security landscape. The threats these changes present increasingly fall to end-users, employees like you, to manage. Below are the most common threats. These are things that you should be thinking about every day.

Passwords

Passwords remain a major threat in 2020. The challenge of passwords is compounded by having so many for all of the various services that you use both personally and professionally. A high percentage of people reuse passwords. This is especially problematic because there are not public breached password databases available on the Internet. These password databases contain passwords from millions of users. If you reuse passwords, there's a good chance they aren't secret anymore. While solutions like two-factor or multi-factor authentication and single sign-on are helpful, passwords remain a significant threat.

Email

Be suspicious of email. We all have email addresses, typically more than one. And those addresses are not hard for attackers to find or for malicious software to guess. Assume your email address is public. And assume that right now there are hackers using software to try to target you via email. The attacks can take different forms - phishing, malware, social engineering - but the common thread is the channel itself - email. If something feels off in email, assume that it is.

Social engineering

Whether via email, chat, support, social, or other channels, you are accessible. Social engineering is a broad term to describe the process of attempting to manipulate you. The goal for attackers it to make money, whether directly through you or through gaining access to your accounts. Social engineering can take tons of different forms - phishing attacks via email or technical support attacks via support tickets or a couple of common examples. It is unfortunately harder and harder to detect when you are benign manipulated. Similarly to email,

maintain a high bar of suspicion and, when it doubt, try to confirm the conversations through other channels.

Privacy (your personal data)

With so many activities online and so many personal devices connected to the Internet, the amount of personal data floating around the Internet is immense. Your personal data can be used in social engineering attacks. Personal privacy is an individual choice but keep in mind that your personal privacy does have a potential impact on the security of your company accounts.

Misconfigurations

With more control over your accounts and sometimes for the products and services you use at work in your hands, misconfigurations are a common threat. It is easy to misconfigure access controls and open up access to company data without realizing it. You may not have a company guide on how to configure every software service you use but, when it doubt, consult somebody in security.

The next several lessons go into detail on best practices you can follow to manage threats and reduce risk to you and your company.

In our brave new connected world, the threats are endless and continuous. Stay vigilant.