Lesson 11 | Security Considerations for Remote Work

Updated 2020-09-14

Remote work, as a trend, has been steadily gaining adoption over the last 10 years. Some notable companies, like Gitlab and Atlassian, operated remote workforces to grow a very large business. But, remote work tipped with COVID-19. Initially forced because of quarantine measures, remote work is now something that many large companies like Facebook and Twitter are allowing, and some are requiring, for the long term.

Whether companies go 100% remote or go remote 100% of the time, the number of employees working remotely is significant in 2020. Remote work changes culture, work habits, and interactions in significant ways. With those changes, there are security considerations that are specific to remote work or at least amplified because of remote work.

Below are remote considerations. Your company may have created specific guides and / or amended its acceptable use policy for remote work. Be sure to check on that.

- **Public wifi.** Computers are constantly connected to the Internet and to connected devices (speakers, peripherals, etc). The types of connectivity are through wifi connections and Bluetooth, most commonly. While there are documented attacks using Bluetooth, this is rare. When it comes to Wifi, there are networks everywhere. You should only join trusted, known networks. This can include coffee shop networks. Be wary of public networks you don't know and that have names you do not recognize.
- **Passwords are even more important**. As remote work mandates remote access to systems and networks, password protections are even more important. Use unique, long passwords.
- **Multi-factor authentication**. With remote work, using multiple factors to secure your accounts and identity are even more important.
- **Secure remote connectivity**. VPNs are easy enough for anybody to use. This, and even secure remote desktop services, can be used to prevent eavesdropping on connections and transmitted data.
- **Meetings and calls in public**. Be cognizant of your location and the content of your conversations. Don't speak too loudly and openly about sensitive company or customer information and data.
- **Zoom security**. Or Meet or Teams security. You should use unique meeting IDs. You can use passwords for your meetings though this does add friction when people join.

- **Screen protector.** You should use a screen protector on your laptop if you use it in public or shared places. This will prevent others from reading what is on your screen.
- **Lock screens in shared places**. You should always lock your computer screen when you leave it. In shared settings, this is imperative.
- **Writing notes**. When in a private setting, like at your desk in an office, you might write down sensitive information and leave it accessible, even if not in the open. In shared or public spaces, be more protective of things you write down.

Remote work is new and strange to many people in 2020. There are lots of positives and negatives to the trend.

Without the physical protection of an office and direct connectivity to company networks, personal security becomes more important to your daily work.