Milima
Security

Best Practices for Telecommuting Securely

In the wake of the pandemic, companies quickly shifted to the work from home program commonly referred to as remote work. This has continued even after the pandemic with many companies going fully remote and others 50% remote.

As with every innovation comes a counter effect, hackers have manipulated all possible avenues to attack companies through remote work. With people being the weakest link in cyber security, there has been an increase in data breaches and phishing attacks.
Did you know that working from home carries additional security risks? There are critical steps your employees can take to ensure they can work remotely from home as securely as possible. Now more than ever, we need to enable our employees to be the best line of defense and equip them with the right tools to combat persistent and evolving cybersecurity threats and risks.

Setting up the Work from Home/ Remote work environment for your organization.

1. Security Team: Coordinate with your security team to gain a better understanding of what key risks you are attempting to manage. We have identified in this guide what we feel are the top, most common risks for a workforce working at home but your risks may be different. A word of caution, a common mistake security teams make is attempting to manage all risks and overwhelm people with numerous policies and requirements. Try to limit the risks you will address to as few as possible. Once you have identified and prioritized those risks, confirm the behaviors that will manage those risks. As already mentioned, if your organization does not have the time or resources for this, then leverage what we document below.

2. Communications: Once you have identified your top human risks and the key behaviors to manage those risks, then partner with your communications team to engage and train your workforce on those behaviors. The most effective security awareness programs have strong partnerships with their communications team. If possible, see if you can even embed someone from communications into your security team. When communicating to your workforce, an effective hook you can use to engage them is to emphasize that not only will this training secure them at

work but enable them to create a Cybersecure home, protecting themselves and their family.

3. Collaboration tools: The other important aspect of the remote work environment is collaboration and communication among teams.To effectively communicate and respond to workforce questions, we highly recommend some type of technology or forum where you can answer peoples' questions, preferably in real time. This can include Google suite chat element, a dedicated email, Skype or Slack chat channel, or some type of online forum such as telegram forum. Another idea is hosting a security webcast that you repeat several times a week so people can pick a time that works best for them and attend the event live, perhaps even ask questions. The goal is you want to make security as approachable as possible and help people with their questions.

Risks to consider with home systems include:

- Multiple users with administrator access allow for download and spread of malware
- Insecure configurations leave the systems vulnerable to attacks
- Home use software installed that are not supported and may not be patched for vulnerabilities
- Institutional information downloaded or cached to the machine may be exposed to other family member

Key Focus training points

Social Engineering

One of the greatest risks remote workers will face, especially in this time of both dramatic change and an environment of urgency, is social engineering attacks. Social Engineering is a psychological attack where attackers trick or fool their victims into making a mistake, which will be made easier during a time of change and confusion. The key is training people what social engineering is, how to spot the most common indicators of a social engineering attack, and what to do when they spot one. Be sure you do not focus on just email phishing attacks, but other methods to include phone calls, texting, social media or fake news.

Strong Passwords

Weak passwords continue to be one of the primary drivers for breaches on a global scale. There are four key behaviors to help manage this risk, listed below. Check out our recommendations about passwords HERE.

- Unique passwords for all accounts
- Paraphrases
- Password Managers
- MFA (Multi-Factor Authentication)

Updated Systems
Another risk is ensuring any technology your workforce uses is running the latest version of the operating system, applications and mobile apps. For people using personal devices this may require enabling automatic updating.

Additional points to consider

- Wi-Fi: Securing your Wi-Fi access point
- VPNs: We recommend using a licenced VPN
- Personal pocket internet access point: This is for individuals who are working remotely but NOT working from home, such as a coffee shop, airport terminal or hotel.
- Children / Guests: To reinforce the idea that family / guests should not access work related devices.
- Detection / Response: Do you want people reporting if they believe there has been an incident while working at home? If so, what do you want them to report and when?

  Reach out to Milima Security for incident response, forensics and Managed Security Services program for continued monitoring.