10 Simple Ways to Lower Cyber Security Risk While Working Remotely

Today, many employees are working from home for the first time in their careers. Whether you have been in the corporate world for 1 year or 40 years, these are tips that should be taken seriously, not only working remotely but also in the office. With the newly found freedom of working from home, it is more crucial than ever to abide by policies and best practices for working from home. With a little additional effort, utilizing the list below can help your company combat this pandemic of malicious attackers.

---

1 Always Connect to VPN

Corporate networks vs home networks differ greatly in the types of security offered. Even with a corporate computer, there are still major cyber security gaps while working from home. One that jumps out is the utilization of Firewalls, many home networks can add firewalls through their home router, however we choose not to activate them. By utilizing the VPN you are able to create an encrypted tunnel between you and the office, which will greatly increase the security of your computer.

2 If Admin, only download needed & trusted applications

The internet is a great tool and there are many great tools available to us for free on the web. While there could be great tools out there and the sources who provide them may be trusted, there could also be known vulnerabilities in the freeware that is downloaded, which can create a vulnerability in the corporate network. If you believe that you need an application, it is always best to check with your IT team about downloading the application.

3 Only use your computer for work purposes

One of the nice parts of working from home is the freedom you get during your normal workday. However, with this freedom comes risks, and these risks must be taken seriously.

4 Only open email attachments from trusted sources

There has been a spike in recent Phishing attacks trying to take advantage of COVID-19, which is a topic all of us are trying to stay well read on. Be careful when you see a new email coming in from an untrusted source, and if you have questions do not hesitate to reach out to your IT team as they would much prefer to catch an email when it comes in over working on an infected computer.

5 Look for consistent misspellings and poor grammar

Not all cyber criminals come from the USA, many of them are found across the world. So, it is quite typical to see misspelling and bad grammar in malicious emails. One thing to note as well is if you start seeing a pattern like this from a trusted source that source may be compromised, you should check that they sent the email before opening any attachments.

6 Check over the actual email address

Many attackers will “spoof” or attempt to hide the identity of their actual email address trying to trick you into thinking that email is coming from a trusted source, such as but not limited to, an email from a high level executive, your IT team, or a manager. Before doing anything with an email, check to make sure that email is actually coming from that person.

7 If IT reaches out, ensure that they are using the normal channels and processes

Most people who work on IT teams are big on processes and ensuring a process is being adhered to, so if you have someone claiming to be part of your IT team asking you to do something that is not typical, such as download a file through email, check with the person whom you think you are speaking with via another means of communication, such as a phone call or through Instant Messenger to ensure it is truly them.

8 Don't hesitate to ask questions

If you think something doesn’t sound right, it usually isn't. Don’t hesitate to ask questions, your friendly IT team is much happier to answer questions prior to a compromise occurring. Remember, there is no such thing as a stupid question!

9 Don't connect to untrusted networks

While many of us are working from home and there are not many options to work from other places than the security of our own residence, there are states that still allow businesses to go on as normal. Cyber criminals are notorious to set up fake networks, so they can see what you are doing. Only utilize networks that are trusted and immediately utilize your VPN to ensure a secure connection to your home network.

10 Always lock your screen while not using your computer

If you get the chance to work remotely in a public space and need to step to the side for a few minutes, always make sure your screen is locked. There could be someone who will do something unwanted to your computer while you are not looking.
Use Windows Key + L to lock.