Working Securely from Home

Russ Burrows, *NDC, Inc. Security Specialist*

The Coronavirus outbreak has quickly moved several office employees to remote employees. As we adapt to the work-from-home lifestyle, we must continue to do our part to safeguard business data and systems. This document provides some basic guidelines to help keep company information safe when you work outside the office.

Summary

The **NDC Security team** recommends you do the following when conducting business electronically from outside the workplace:

1. Install and run anti-virus, anti-malware and a firewall on your personal computer. Windows comes with free tools that you should use.
2. Do not use unsecured wireless networks.
3. Do not keep company files and documents on your home computer.
4. Be conscientious of the sites you visit and the programs you install and use. Your computer can become the entry point used by hackers to enter your company network.
5. If you deal with sensitive company data, remember to keep it private at home as well. Lock your computer when not in use. Friends, relatives and roommates who are curious about your job are not entitled to see your company information.
6. Contact your company IT department if you have questions or issues.

Home Computers

There are now many employees utilizing their home computer instead of a company-provided one. Company-provided computers usually come with a set of security-related products including anti-virus, a firewall and malicious software (a.k.a. “malware”) protection. If you are using a home computer for work, it needs to use the same types of products to avoid data loss or leakage. Windows computers come with Windows Defender for anti-virus, and Windows

Defender Firewall for blocking unwanted traffic. *Please validate that these services are running on your home computer.* Contact your company IT department if you are unsure how to do that. If you don't have an anti-malware program running on your home computer, there is a free malware scanning and removal tool called Malwarebytes that can be downloaded here.

The **NDC Security team** recommends scanning your computer daily for any new viruses and malware.

Unsecured Wireless Networks

When working outside the office and searching for a wireless network to use, you will often see wireless networks connections that do not require a password to use them. These open, unsecured wireless networks are not okay for business use. These networks transfer data without any encryption, and company information traveling on these roads of Internet superhighway can be seen as easily by cyber criminals as what you see out your car window when driving down the street. The **NDC Security team** recommends not connecting to unsecured wireless networks. If your home network is currently open, please set up authentication on it.

Exposing Sensitive Corporate Data

Wondering whether to move an electronic file, document or data from the company network to your home computer? Resist the urge to do it. When data is moved to your home computer, it can no longer be protected by all the measures your company has in place to protect it while it lives in the corporate network. The **NDC Security team** recommends to not move company information over to your home computer, if possible.

Avoid the "Over the Shoulder" Transfer of Sensitive Information

Remember that business data that you access at home may be accessible to every person who lives in or visits your home. Friends and roommates who are curious about what you do at work should not have the opportunity to view or access company information. While at home, like at work, lock your computer when you are not using it. Disconnect from the company network when your work is complete for the day. Know who is around you, and let them know your work is confidential and to respect your privacy.

And Finally…

If you have technology-related questions or issues, contact your company IT department right away. Don't take any unnecessary risks.