Can We

Work From Home (WFH) Securely?

In the past month or so, most people practicing social distancing by staying home have had to rely on remote access tools to accomplish what used to be a normal daily office routine.

The massive growth in Work From Home (WFH) teleworking has been sudden and companies like Zoom have seen usage explode. In addition to business and government organizations, school systems, churches, families, and friends all over the world are now using laptops and smartphones to stay in touch with one another.

These platforms are also experiencing heavy media scrutiny of their security features and many are concerned about the risks. Is there a right way to use this technology safely?

Before attempting to answer that question, let's consider the driver that led to WFH: millions of employees affected by the COVID-19 quarantine. Teleworking is essential to the survival of these organizations, so undoubtedly a fundamental need is being solved. Accountants, sales professionals, engineers, and just about anybody with a job that involves a desk and a computer has been relocated to their home. This has led to at least one or two awkward moments for all of us, as people join virtual meetings and forget where the mute or video disabling buttons are, and what exactly is appropriate WFH work attire anyway?

As the novelty of this massive cultural shift wears off for most businesses, some questions remain unanswered, and people are right to wonder if

"People are right to wonder if the technology they are using to work from home is as secure as what they used in the office."
-Jason Ingalls

INGALLS INFORMATION SECURITY

Cyber Innovation Center (CIC)
6300 Texas Street, Ste. 240, Bossier City, LA 71111

WWW.IINFOSEC.COM
(888) 860-0452

the technology they are using to work from home is as secure as what they used in the office.

Let's cover some basic ground rules so that we can all help protect our information while working from home.

Multi-Factor Authentication (MFA/2FA)

Now that most people are connecting remotely to computer systems hosted either in the Cloud or in a server at the office, it's critical that their account credentials are protected with Two-Factor Authentication (2FA) or Multi-Factor Authentication (MFA). This advanced form of authentication is now an essential requirement for all remote access credentials. As long as an account has 2FA/MFA enabled, if a username and password are stolen they are useless without the additional factor of a code, certificate, or other MFA asset that must be present. Your IT Manager can help you set up your advanced authentication solution if you don't already have it configured. **For those who haven't set this up yet, don't wait!**

Virtual Private Network (VPN)

Virtual Private Network connections allow home workers to connect into their office network, Cloud-based network, or any other computer network through the Internet safely and securely. If you need to access a work computer remotely using the Remote Desktop Protocol, it should never be exposed to the Internet but rather accessed via a VPN. VPN login credentials should have 2FA/MFA enabled.

What about Video Teleconference, can it be Secure?

Now that we have discussed secure ways to access our systems, what about communicating with folks virtually face to face? Can we do that securely? **The answer is an absolute yes!**

Understandably, there is a lot of fear about using popular video teleconferencing software because the default configurations are not always secure and the user must take additional steps to enable the necessary security settings. Fortunately, vendors are responding quickly, eager to show they are listening to their customers and are readily making available articles on how to enable security, so **what do we need to do to ensure our video chats are secure?**

The simplest way to securely video chat with your coworkers is to require a password for any meeting. The meeting password should be shared only with the meeting participants.

There are other security settings options that you can enable on most popular video conferencing systems, including:

- Ensure that only the host can share their screen by default
- Ensure that remote control is disabled
- Ensure that the host is locked to a single participant
- Do not allow "Start before leader arrives" and instead use "Waiting rooms"

By using advanced security on your credentials and on your communication tools, and by making sure we follow some simple rules, we can all get back to work securely even if we are new to the WFH phenomenon. If some of the terms or concepts covered in this blog seem foreign to you, reach out to your IT manager and ask them. They will help you understand whether or not you are already doing these things, and if not, when you can expect to.

INGALLS INFORMATION SECURITY

Cyber Innovation Center (CIC)
6300 Texas Street, Ste. 240, Bossier City, LA 71111

WWW.IINFOSEC.COM
(888) 860-0452

Stay safe, stay home and stay productive!

Questions about how to stay secure while working remotely? Ingalls helps businesses large and small manage security risks and defend against cyberattacks. If you'd like to learn more, please contact us here. One of our cybersecurity experts will be more than happy to assist you and answer any questions you may have.

A Trusted Advisor & Service Provider

Since 2010, Ingalls Information Security has been in the war rooms and board rooms of Global 2000 companies, investigating computer networks targeted and attacked by criminals and nation-state sponsored hackers. This experience gives us an edge in preventing and responding to cyberattacks, as well as developing risk management strategies for our clients. We work for high-profile clients in many different industry verticals, from multi-national conglomerates to small businesses that are increasingly vulnerable to cybercrime.

INGALLS
INFORMATION SECURITY

Cyber Innovation Center (CIC)
6300 Texas Street, Ste. 240, Bossier City, LA 71111

WWW.IINFOSEC.COM
(888) 860-0452