Cyber Security Tips - Focus on working safely from home

Introduction

Just like that, COVID-19 has changed our regular cadence of getting up in the morning and going into the office to work. Most of us are now working from home, and even those still out working on the front lines are relying on their phones and laptops to stay connected with loved ones.

Unfortunately, there are bad actors (people with malicious intent) looking to take advantage of vulnerable workers during these uncertain times. Risks around data and identity theft, ransomware and insider threat need to be understood and appropriately managed. As a community of security professionals, it is our responsibility to make sure that companies and the people they employ are equipped with the necessary tools and knowledge to promote a safe and secure working environment, both inside the office and at home.

In this article we look at some of the biggest risks to privacy and information security for teleworkers, along with best practices for minimizing risk.

BEST PRACTICES WHEN WORKING FROM HOME

DO	DON'T
Use a VPN	Use free WiFi unless you have a VPN
Use antivirus and firewall protection	Allow "IT" to access your computer without verifying their identity
Use a password manager	Use your personal email for work purposes
Beware of COVID-19 phishing scams	Click on links (email or text) without verifying the source

The tools listed below are used by the authors and are not an endorsement of any company or product. They are intended for use by readers who do not have an IT team support infrastructure. They are in no way intended to replace tools recommended and incorporated by your organization's IT team.

1. Use a VPN (Virtual Private Network) to access company files

What is it?

A Virtual Private Network is a tunnel that creates a network-within-a-network to keep your information private when communicating via the internet.

Why do I need it?

If you are working from home and your family are all using the WiFi, you want to keep your work data separate from the other activity. A VPN keeps your data contained within a secure tunnel on that WiFi. This is a best practice when using a shared network at home, and a necessity whenever you use free WiFi connections. Free WiFi, even with a password, is very susceptible to bad actors who can monitor traffic to obtain your personal information and data.

PC Magazine[1] lists the top 10 VPN services for 2020. The table below summarizes some of the products recommended specifically for new or home users.

VPN service providers	Ranking for general use	Free version?
NordVPN	Best for general users	30-day money-back guarantee
TunnelBear*	Best for first-time users	Yes, with limitations
CyberGhost	Best for general users	14-day money back guarantee

***TunnelBear VPN** – (Rated best for first time users) Sherri Ireland says it is user friendly and can be used on your cell phone and computers. Free version with limited bandwidth, pricing for monthly and annual options are reasonable. https://www.tunnelbear.com/

The Wirecutter[2] outlines trust considerations for consumers when selecting a VPN service.

2. Consider malware protection with advanced antivirus and home firewall

What is it?

Antivirus (AV) software prevents known malware or malicious code from running on your system and changing the way your computer works. Antivirus programs need to be updated regularly — most are automatically updated daily or weekly. It's important that these programs are kept up to date, as this is how new viruses are detected.

A firewall protects your computer and private network from threats on the Internet. It can be configured to block data from certain websites or applications, while allowing relevant and necessary data through.

Malware is most often inadvertently loaded onto your computer when you click on a malicious link. It may be an advertisement on your favourite social media platform or a website that contains malicious code.

Why do I need it?

There are many instances of viruses that can impact your computer, changing the way it works, potentially stealing sensitive information, and potentially locking you out of your computer permanently. Computers that are used at home and connected to a company network are of paramount concern as an infected computer can affect the entire company network.

PC Magazine[3] lists the best antivirus protection for 2020. This table below summarizes some of the products recommended in PC Magazine specifically directed for new or home users.

Antivirus providers	Ranking for general use	Free version?
McAfee AntiVirus Plus	Best for multi-device household	30-day money-back guarantee
Norton Anti VirusPlus	Best for single desktop protection	14-60-day money-back guarantee depending on plan purchased
Trend Micro	Best for single desktop protection	30-day money-back guarantee

Windows Defender (free to Windows users and has antivirus and firewall) and **Malwarebytes** (for Windows and Mac) – Sherri Ireland uses this combination of protection. Malwarebytes has a free version to try and there is an annual subscription service that is reasonable. https://www.malwarebytes.com/

[1] The Best VPN Services for 2020, https://www.pcmag.com/picks/the-best-vpn-services
[2] The Best VPN Service, https://thewirecutter.com/reviews/best-vpn-service/#trusting-a-vpn
[3] The Best Antivirus Protection for 2020, https://www.pcmag.com/picks/the-best-antivirus-protection

3. Use a Password Manager

What is it?

A password manager allows you to keep all your passwords in one secure (encrypted) location. It also assists with generating complex passwords for new logins. You'll only have one password to remember to access your user logins and passwords.

Why do I need it?

Some people are reluctant to have a password manager, or to put all their passwords in one online location. While that is understandable, it is a much better alternative to writing your username and password down on paper or reusing the same password for multiple sites. Password managers can also generate complex passwords which you don't need to remember, helping you stay safe online.

PC Magazine[4] lists the best password managers for 2020 specifically for new or home users. PC Magazine[5] also published a list of the best free password managers for 2020.

Password managers	Ranking for general use	Free version?
Soho Vault	3.5 out of 5	Yes, with limitations
Dashlane	3.5 out of 5	Yes, with limitations
Keeper Password Manager & Digital Vault	3.5 out of 5	Yes, with limitations

RememBear – Sherri Ireland uses RememBear as her password manager: https://www.remembear.com/

4. Social Engineering and Anti-phishing Tips:

Phishing, spear phishing, vishing, pharming… these are all ways in which cybercriminals use social engineering to deceive and manipulate individuals into divulging confidential or personal information for fraudulent purposes. Social engineering attacks are most effective when they target individuals with privileged access to sensitive information such as private login credentials or credit card information.

In the wake of COVID-19, a strained healthcare system and faltering economy have led to increased anxiety and vulnerability amongst workers, making them more susceptible to COVID-related phishing scams. A CBC report published March 30, 2020[6] showed that phishing scams increased by 600% between February and March this year. These kinds of attacks can happen over the telephone ("vishing"), via text message ("smishing"), targeted email ("spear phishing") using compromised social media accounts, or fraudulent websites ("pharming"). Regardless of which method is used, there are some common giveaways that will help you identify a "phish"[7]:

I. Look for a generic greeting.

Phishing emails are typically sent out to the masses. As a result, the attacker might use a generic greeting, such as "Dear member" or "Dear Acme Bank customer".

[4] The Best Password Managers for 2020, https://www.pcmag.com/picks/the-best-password-managers
[5] The Best Free Password Managers for 2020, https://www.pcmag.com/picks/the-best-free-password-managers
[6] Email, text message attacks surge during COVID-19 crisis, https://www.cbc.ca/amp/1.5513315
[7] Source: ADGA Advanced Cyber, Intelligence and Security (ACIS), https://www.adga.ca/converged-security-solutions

II. Check the Sender's email address.
A common tactic used by cyber criminals is to pose as someone you know. Always check the Sender's email address in the "From" field of the email headers for any unusual words or spelling in the domain name. For example, an email phish might be sent from the address "promotions@amazan.ca" instead of a legitimate "@amazon.ca" address.

III. Determine if there is a call to action.
The goal of most phishing attacks is to get sensitive information. Cybercriminals like to do this by posing as a legitimate financial institution and asking you to update or verify your information. Most real banks would never send such a call to action by email.

IV. Analyse the email/text message for a sense of urgency.
A common tactic to get you to fall for a phishing scam is to create a sense of urgency. There is almost always a problem that requires your immediate attention.

V. Look for an embedded hyperlink or attachment.
Many phishing emails include hyperlinks with deceptive URLs (a URL is the address starting with https://www.). The displayed URL might be legitimate, but when you hover your mouse cursor over it (without clicking it), you might discover that the actual URL does not match the displayed information. These deceptive links can take you to fraudulent websites that can be used to trick you into entering your personal or sensitive information or to websites that will install malware on your computer.

If there is a file attachment, opening it will result in malware being installed on your device with or without your knowledge. Legitimate organizations typically do not email files out of the blue. Unless you specifically requested a document from an organization, be wary of any attachments. Similarly, be wary of attachments emailed by individuals if you did not request the file.

5. What about the Insider Threat?

Traditionally, one would think about the Insider Threat as a disgruntled employee who harbours malicious intent to steal information or damage company property. Now, with social engineering attacks on the rise, it's often the well-intentioned and untrained employee who poses the biggest threat to an organization.

A lack of policy enforcement and regular training on security awareness can mean that employees with coveted login credentials are more easily tricked and exploited by cyber criminals who are looking for an easier way into our private networks. Reference this whitepaper[8] by ASIS Women in Security Publications Committee to learn more about the Insider Threat and how to minimize risk exposures for yourself and your company.

6. Conclusion

COVID-19 is an unprecedented challenge for all of us. As we adapt to new ways of working, and our homes become common sites of potential workplace cyberattack, we need to stay vigilant about both new forms of threat and the longstanding methods bad actors are beginning to employ with more frequency. Thankfully, the most effective first line of defence is the use of common sense. The tools outlined are easy to use, readily available, trustworthy and proven. We encourage you to share this article with your family, friends and coworkers.

[8] https://www.womeninsecurity.org/single-post/2019/11/28/Key-Considerations-When-Building-Your-Insider-Risk-Program

Authors:

Isabelle Hertanto

Isabelle Hertanto, CISM, is a dedicated technology professional, with over 15 years of experience in the security and intelligence industry. As Senior Cyber Security Lead for ADGA Group Consultants Inc., Isabelle delivers managed solutions and services to organizations in IT security governance, risk management, and compliance. She is an instructor within the Cyber Security Management program at the University of Toronto, School of Continuing Studies and is a member of the ISACA Toronto Chapter.

Sherri Ireland

Sherri Ireland, CISSP, is a 30-year veteran of the security industry. In 2015, she started Security Exclusive, providing recruiting, cyber awareness training sessions and security consulting. She is part-time faculty in the Protection Security and Investigation program at Fleming College since 2011 and the Vice-Chair of the ASIS Toronto Chapter 193.