Work from Home Safely

5 BASIC TIPS

More people are being asked to work remotely than ever before. This shift leaves us open for people to take advantage of how the security landscape has changed for businesses. To help protect yourself and the organization, here are some tips for maintaining good cyber security.

QUICK

DATA BREACH STATISTICS

In most cases, it takes companies about **6 months to detect a data breach.**[1]

61%
of data breach victims were companies with **less than 1000 employees,** in 2017.[2]

65%
of companies have over 500 employees who have **never changed their password.**[3]

95%
of data breaches have cause **attributed to human error.**[4]

5 TIPS FOR

MAINTAINING GOOD CYBER SECURITY

01 YOU ARE THE MOST POWERFUL DEFENSE.

Phishing is still the number one means of system compromise so don't just click on anything that comes across your screen. Be cautious of emails and websites you are unfamiliar with. Be careful when installing applications as they should always come from a trusted source. If you need to install a new application or service and are not sure, check with your IT department for approval. They can get you trusted sources and steer you clear of potential threats.

02 UPDATE, UPDATE, AND UPDATE.

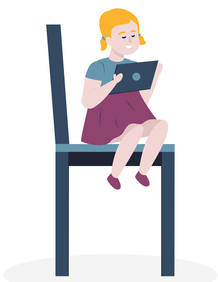
Would you like to protect against 95% of the known vulnerabilities? If so, keep your systems up to date, that's all it takes. The trick to this is to not only keep the operating systems up to date, but also the malware protection, applications, phones, home firewall, and home devices. If it connects to wireless or ethernet, make sure it is up to date. As you look for devices on your home network, you will find more than you expected. Take a simple inventory while you are at it since it is always good to know what you need to update again later. IT Pros always want to know exactly what is on their networks and you should too.

03 PASSWORDS MATTER.

Change any default passwords and make them difficult to guess. If you have a device like your home router or security panel, make the password 15 characters or better. This will make it hard to compromise. Commonly accessed devices should have 11 characters or better to make it difficult. String 3 or 4 short words together to make a silly phrase like BlueBunnyPencils. This is a very effective means of protecting your systems. Never leave the default password unchanged for any device. If you can't change the password, put it on the guest network.

04 PROTECT YOUR SYSTEMS.

Every device connected to your network should have protections. Malware protection is a great tool for your computers and phones. Home routers should have a built-in firewall. If they don't or are over 5 years old, replace it. The technology, power, and capability of the new devices is easily worth the cost. With the explosion of smart devices, you need top notch protection.



05 USE MORE ADVANCED STRATEGIES.

Most new firewalls will let you separate stuff on your network. Set up the guest network and use it. Put the kids, Xbox, friends, and non-essential devices on the guest network. Your home network is now a business network, treat it like one. If you are able to keep your computer dedicated for work, consider it. Children are very curious and often don't have the awareness to understand the perils of that great new free app they just installed. If your organization or client has VPN, use it. This encrypts traffic and directs it through more sophisticated protections. Take some time to harden your firewall by turning off services you don't need. It will take a little work but worth the time. The Center for Internet Security has a brief guide that is very helpful titled "Telework and Small Office Security Guide".

Cyber security is important to your business when you are in the office and it should be the same now that you are working from home. ***Take a little time to protect your home and business so you can focus on what really matters.***

moser consulting
MOSERIT.COM

[1]Source: ZD Net (https://www.zdnet.com/topic/cyberwar-and-the-future-of-cybersecurity/)
[2]Source: Verizon (https://enterprise.verizon.com/resources/reports/dbir/)
[3]Source: Varonis (https://info.varonis.com/hubfs/2018%20Varonis%20Global%20Data%20Risk%20Report.pdf)
[4]Source: Cybint Solutions