Working Securely from Home

Description

As we have all been faced with challenges during COVID-19 changing the way we do business with many of us working from home, hackers have been presented with opportunities to cast a wider net on attacks. IT security has always been important and during these times that importance is even greater.

In an ideal world we would have had time to plan on how to securely make the transition from employees working in the office to working from home. Unfortunately, many of us made the transition with little to no time to plan. Now that the dust has settled a bit, although the future is still uncertain when and if we will go back to doing business the way we used to, it is a good time to confirm that employees working remotely are doing so as securely as possible.

Below are some tips on working securely from home:

- Employees should follow the same policies and procedures as if they were working in the office.
- If possible, have a private area set up to work.
- Connection to the office should only be made using a secure VPN (Virtual Private Network).
- Passwords used should be unique and no less than 12 characters on all devices being used, the longer the better.
- Employees using a personal computer/laptop should make sure there is up to date anti-virus software installed and the operating system is up to date with updates/patches, including 3rd party software, downloaded and installed on regular basis.
- If using a wireless connection, make sure the connection is encrypted and the wireless password is strong.
- Confirm that the login and password for the router (usually provided by the ISP, Internet Service Provider) has been changed. Most routers in homes still have the default login and password which is not only weak, but also known across the Internet and easily searchable.
- Lock your computer/laptop screen when you walk away or are finished working.
- Only use company set up email, messaging, storage, etc when doing work for the company.
- Stay vigilant when it comes to phishing emails. Phishing emails are up 667% and according to Google 81 million phishing emails containing malware are being sent each day. Verify, Verify, Verify before providing personal information or doing a financial transaction.
- Notify your IT company IMMEDIATELY if you possibly clicked on or downloaded something suspicious. The quicker they can run mitigation the better.

As many of you are aware hacking is big business costing many businesses a ton of money. Many hackers are employed just like we are. They are given quotas to meet, deadlines, and are expected to perform in order to keep their job. Letâ??s make it hard for them to stay employed!

SME is here to assist in any way that we can. If you have any questions about working securely from home or any other IT/security related questions please give me a call at 703-378-4110 or email melissa.ellis@smeinc.net.

Stay Safe, Healthy, and Sane!

Melissa Ellis, VP/CFO

Melissa Ellis is a co-owner of Systems Management Enterprises, Inc. (SME). SME is a Virginia based Information Technology and Security Company providing data center services, managed security, compliance solutions, and technical support to businesses nationwide.

Melissa has worked with businesses in the financial, medical, and professional services industries in a support and training role. Over the last several years she has specifically worked within these industries on compliance initiatives and provided security awareness training. Melissaâ??s background includes studying Criminal Justice at Radford University and obtaining a better understanding of compliance by becoming a CHP. Melissa is passionate about educating businesses on how they can put the necessary layers of protection in place to safeguard their data.

Category

1. Cybersecurity

Date Created
2020/06/02
Author
vltaexaminer