



WORKING FROM HOME.
LEARNING FROM HOME.

Staying Secure From Home

One PPG Place, Suite 1700
Pittsburgh, PA 15222
(412) 697-5200
www.schneiderdowns.com



SCHNEIDER DOWNS

Big Thinking. Personal Focus.



Staying Secure From Home

As we enter the fourth quarter of 2020, the new normal has simply become normal as the entire country continues to adapt to working and learning from home during the COVID-19 pandemic with a recent survey reporting nearly [51% of employees](#) in the United States are working remotely. In addition, the report predicts that even in a post-pandemic environment the remote workforce will be 30%, nearly triple the amount reported pre-pandemic. Organizations across the globe including Twitter and Nationwide have already installed permanent work from home policies going forward and the start of the academic year continues to add to the need to understand and implement security best practices at home and on the go.

In support of [National Cybersecurity Awareness Month](#), we asked our team of experts to reflect on the continued state of remote workforces and share best practices to help organizations and individuals mitigate risk from the top down.

Enforce Multi-factor Authentication

One of the oldest and strongest security tools continues to be the use of multi-factor authentication (MFA), both in personal online accounts and end user security. Simply put, MFA is a digital authentication method requiring users to confirm two or more pieces of evidence to access online accounts. A popular form of MFA is known as two-factor authentication (2FA) which requires a combination of actions to provide access which usually consists of a password and code provided by an app or physical device. There are number of apps that provide this protection including Google Authenticator, DUO and Microsoft Authenticator, as well as older methods which send codes to a physical tokens provided to users.

Pro Tip!

Provide clear instructions to users on how to setup MFA protection on their devices.

Use Virtual Private Networks When Possible*

During the initial shift to the remote workforce, one of the most discussed security terms was virtual private networks (VPNs). From IT teams across the country doing impromptu stress tests to assess if they could support a completely remote workforce to workers being reminded to always use theirs, VPNs continue to be one of the most effective and important security tools available to organizations. VPNs are designed to provide an encrypted channel to transmit data between remote users and company networks in a private and secure manner, which has become a top security need with the increase of remote workers using personal Wi-Fi to access company servers this year.

**The protections provided by web filters and other on premise security products often require a full tunnel VPN to provide those services to an employee computer outside of the office. If a split tunnel VPN is in use, an employee's internet traffic will route out of their local internet connection and not the corporate firewall, negating any organization defensive measures at the internet level. It is important to ensure that enough internet bandwidth exists for using a full tunnel VPN if you are currently in split tunnel mode and you plan to switch.*

Further, many businesses now use a range of software as a service (SaaS) platforms, such as Salesforce, Office 365 and etc. and the traditional need for internal access to company resources may be limited or none existent at some organizations. If you are an organization with a decentralized platform, ensure that your host based and cloud services

protections provide the same level of protection a typical corporate network would provide, such as web filtering and strong antivirus/Endpoint Detection and Response (EDR) software.

Pro Tip!

Secure access to VPNs with strong password requirements and multi-factor authentication!

Install Patches and Updates

The importance of installing patches and updates is nothing new, but continues to be one of the most overlooked security measures impacting organizations and with the amount of workers at home, neglecting updates can lead to significant risks. Software updates and security patches are critical in keeping your information secure and operating system current, in addition to reducing vulnerabilities, which is why choosing to click on “install updates now” when the reminder pops up instead of “remind me later” is so important, both on work and personal devices.

Pro Tip!

Send communications for scheduled updates or setup automatic updates if possible.

Keep Work and Personal Devices Separate

The old adage of keeping your personal and work life separate also applies to working remotely on company devices such as laptops and phones. When using company equipment, be cognizant of using it strictly for work as even simple browsing such as online shopping or the latest sports article can lead to security issues that can directly impact not only the device, but the security of an entire organization.

With a recent survey showing that [56% of workers are using their personal computer for work](#) and 42% are using their personal phone for work, the need to understand and address BYOD (bring your own device) risk is another security concern to take into consideration. BYOD policies usually take form when a company offers to reimburse employees for using their personal devices for work and in best case scenarios requires employees to install administrator controls and security measures on their personal devices



(smartphone, tablet, etc.) to allow a secure connection. The increase in BYOD during the pandemic has created an additional layer of risk, with the same survey reporting 23% of employees didn't even know what security protocols or software were in place on their device they were using for work.

Whether your organization is providing devices or offering BYOD options, be sure to develop and enforce security policies which meet industry requirements, acceptable use guidelines and best practices. In addition, there are software options out there for mobile software and data security.

Pro Tip!

Ensure all devices with network access have security solutions installed and encrypted!

Communicate Security Policies

One of the most effective ways to strengthen your security posture is to educate your end users on company policies, procedures and best practices. Communication is especially important this year, with the massive shift to remote work accommodations and the inherent security risks that come with. A recent survey shows [49% of employees working at home due to the pandemic are doing so for the first time](#). The same survey also shows that 75% of those working at home usually or almost always follows IT advice and while that percentage sounds high, it only takes one user to compromise an entire organization. Clear and consistent communication can be the difference between end users being your biggest liability or your strong security advocate.

Pro Tip!

Regularly share security policies, resources and contact information with your team. Even better, take employee behavior out of the equation by enforcing policies via technical controls wherever possible.

Secure Your Personal Network

The days of your home Wi-Fi being just for Netflix and web browsing use are long gone in 2020 with our homes acting as offices and classrooms for many, which is why keeping home networks secure is so important. When setting up your network, be sure that your connections are secure and private, and also monitor your Wi-Fi connection strength. With entire families now working and learning from home, Wi-Fi strength can be understandably spotty, which aside from being inconvenient can impact the overall effectiveness of antivirus and end point detection tools.

Add additional security to your router with a product such as [Disney Circle](#) or [Firewalla](#) which can provide easy to use parental controls and additional security.

Pro Tips!

Be sure to change your router name and Wi-Fi password from the default settings.

Safely Work from Anywhere

As the country opens up, many workers have become accustomed to working remotely and are venturing out of their home office lending to the trend of [working from anywhere](#) which has added a sense of flexibility in a stressful time. Whether you are working from the local coffee shop, at the beach or even visiting with friends



and family, your security standards must stay the same. When traveling it is always best to always use a VPN if possible and avoid public Wi-Fi as you never know who set it up, if the connection is legitimate and who else is connected. Even if you are at a trusted space with friends or family, that does not mean their home network is secure. And as always be sure to keep physical security top-of-mind when traveling anywhere with your devices as stealing a device is easier than trying to breach it digitally.

Pro Tip!

Check with your IT Department for policies when working off-site or traveling.

Don't Improvise

The shift to working and learning from home has introduced a number of online platforms to keep us connected including Zoom, Microsoft Teams and Google Classrooms, all of which came with some sort of learning curve for the users. With the increased reliance on new software and tools, be sure to communicate to your users what platforms are approved for use when connecting to your network and monitor employees to ensure they are only using business-related plugins and web extensions.

Pro Tip!

Ask organizations for a list of approved websites, applications and best practices for safe usage.

Secure Password Management

With the number of devices, applications and sites being accessed for work and school, remembering passwords can be understandably overwhelming which can lead to some bad security habits. And being at home may lead to a false sense of security where that sticky note you used to hide under your keyboard at work is now open on the kitchen table or accidentally thrown away. Even if you securely store your passwords, if a site you visit is part of a breach, chances are your passwords are out in the wild. To help secure passwords and ease the burden of remembering all of them. One powerful tool for password security is password management software, which essentially acts as a master lock for all of your passwords. Password managers not only add a layer of convenience to password security, but many help you create strong

passwords with stringent requirements. Always enable multifactor (MFA) authentication for password managers to ensure that your password vault is the most protected it can be.

Pro Tip!

Many password management software providers, such as LastPass and 1Password, offer options for personal and enterprise security needs.

Avoid COVID-19 Scams

In addition to targeting the large scale remote workforce, cyber criminals predictably used the global pandemic to craft countless COVID-19 themed attacks to take advantage of users letting their guard down due to the shift to remote environments and uncertainty of the new normal. From the initial reports of tens of thousands of domains with the words Coronavirus/COVID-19 being purchased starting in January and the steady flow of fake CDC emails, malicious COVID-19 tracking websites, phishing emails and stimulus scams, the global pandemic provided a fresh coat of paint for some of the most common attack methods including phishing, smishing and web-based malware attacks.

Pro Tip!

Share the [FTC Coronavirus webpage](#) to educate others on the warning signs and best practices to avoid COVID-19 scams.

Learning from Home

With the start of the academic year, schools and universities across the country have introduced a

number of remote learning schedules and options which has introduced a number of security issues for students, teachers and administrations. When learning from home, be sure to verify what resources are approved for use and make sure to use trusted sites to ensure you aren't compromising your networks with malicious plugins, downloads and web-based attacks. This is especially important for college students who may be looking for a free version of a textbook or doing research outside of the approved library search engines and databases. For the younger students, be sure to secure devices kids are using for school, ideally restricting their ability to download web applications and access to suspicious sites with parental controls. And while the thought of learning from home securely may feel daunting, especially parents with younger students, the same best practices to working from home apply to learning from home. Products mentioned previously, such as Disney Circle and Firewalla can help accomplish some of these security measures in consumer/home networks.

Pro Tip!

Contact the school district or university for a list of approved websites and applications.

Experiencing or suspect a network incident?

Contact the Schneider Downs [Incident Response Team](#) 24x7x365 at 1-800-993-8937.



Related Resources

Our team has published a number of resources throughout the pandemic to help keep security top-of-mind, all of which are available for open access:

- Infographic – [Identifying and Avoiding COVID-19 Scams](#)
- Whitepaper – [Securing a Remote Workforce](#)
- Our Thoughts On Article – [Coronavirus Cyber Scams are on the Rise](#)
- Our Thoughts On Article – [Best Practices for Working from Home During the Pandemic](#)
- Our Thoughts On Article – [Evolving Cyber Threats of the New Normal](#)

How Can Schneider Downs Help?

Schneider Downs can help your organization to be better prepared. We offer a comprehensive set of information technology security services, including network penetration assessments, network vulnerability assessments, web application security testing and IT security maturity assessments. Our team of network security specialists, application configuration specialists, implementation consultants and certified information system auditors provide a growing slate of services dedicated to keeping organizations secure, including:

- Digital Forensics and Incident Response
- Enterprise Information Security Program Review and Consultation
- External Footprint Analysis
- Firewall Configuration Review
- Forensic Analysis
- Incident Response Plan Development, Testing and Training
- Indicator of Compromise Assessment
- Information Security Program Maturity Assessments
- Infrastructure Assessments
- Intrusion Prevention/Detection Review
- MS Office 365 Security Assessments
- Penetration Testing
- Phishing Simulation Exercises
- Purple Team Assessments
- Ransomware Security Service
- Recovery and Remediation
- Vulnerability Assessment
- Web Application Penetration Testing

Contact Us

cybersecurity@schneiderdowns.com
www.schneiderdowns.com/cybersecurity

Want to be in the know? Subscribe to our bi-weekly cybersecurity newsletter at www.schneiderdowns.com/subscribe.