10 SECURITY BEST PRACTICES

When Working Remote

OnCourse Learning

In partnership with

SBS CyberSecurity

10 Security Best Practices When Working Remote

Written by OnCourse Learning, in partnership with SBS CyberSecurity

Due to the private information within the financial service industry, working remotely isn't typically something all employees can do.

However, there are situations when it does make sense for individuals to complete their jobs outside of the brick and mortar of a company. As in all working environments, there are pros and cons to working from home. When working remotely, security is a top concern for companies, especially those in the financial services industry.

TABLE OF CONTENTS

What to Expect

OnCourse Learning has partnered with SBS CyberSecurity to provide the top 10 security best practices when working remote.

U.S. companies with employees who worked remotely saved **$5 billion**[2]

Pros & Cons of Working Remote

PROS

Productivity

When working in the right situation, it is proven that remote workers can be even more productive. A two-year study by Stanford University[1] found that there was an impressive increase in work productivity among people who worked from home.

Reduction in Costs

An organization will benefit from a reduction in overhead costs when it comes to remote working, as well as costs related to unproductivity. In 2018, there was an estimated $5 billion[2] in cost savings for U.S. companies with employees who worked remotely - and that's just counting part-time workers. Employees will also save an average of $7,000 a year[3] from reducing or eliminating the cost of commuting, food, clothing and childcare.

Flexible Hours

Depending on the role and demands of your financial institution, working from home allows some flexibility in the hours your employees work. Having time to tend to responsibilities can help reduce stress, especially during uncertain and naturally stressful times. Allowing employees to have a flexibility schedule, can increase employee retention, which also increases company productivity.

CONS

Less Collaboration, More Isolation

Conversations that happen naturally in the office, or casual collaboration, cannot be replaced when working remotely. For some, isolation can make you more productive. For others, working in the office allows employees to build important relationships and meet new people.

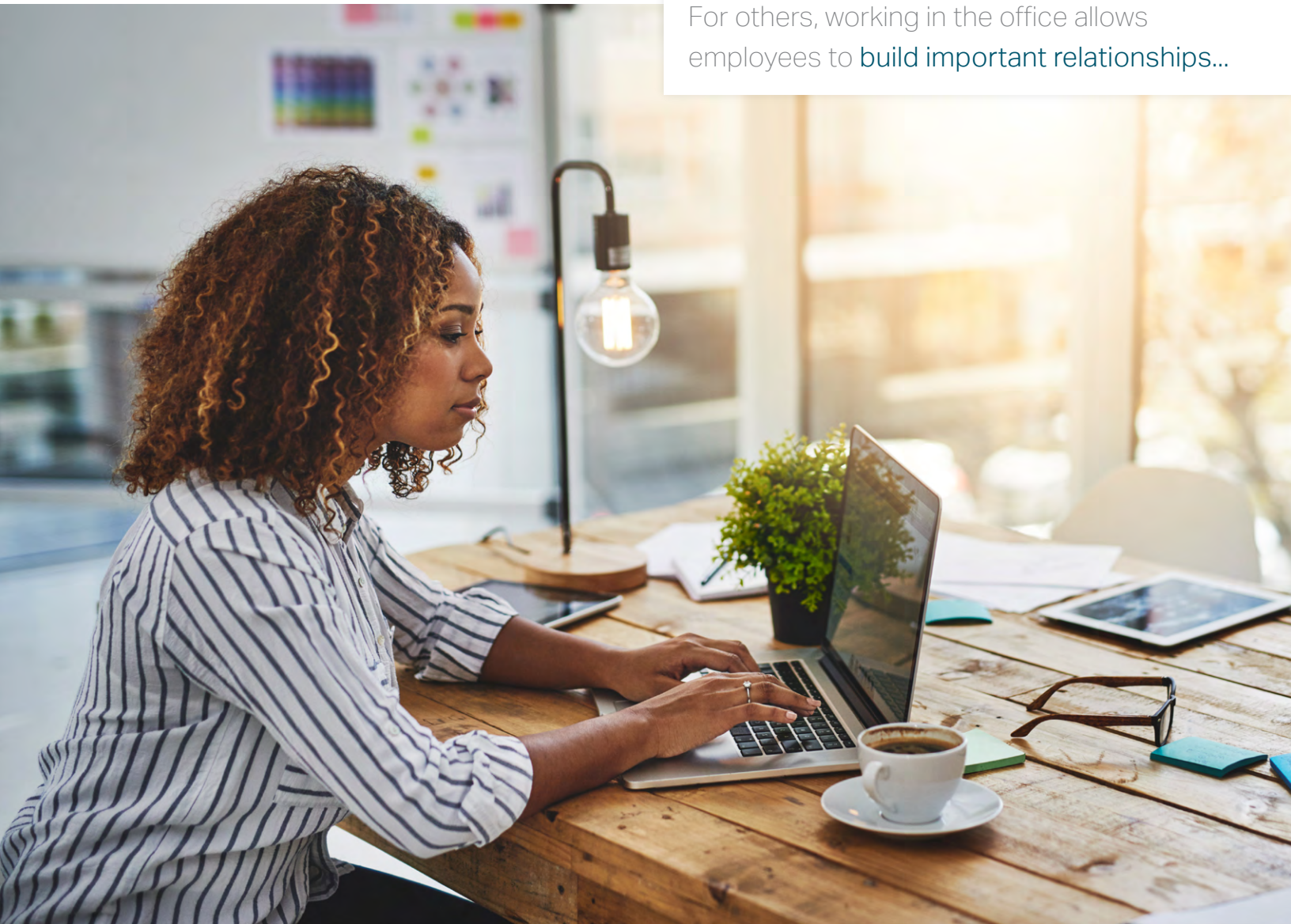
Less Control Around Cybersecurity

Public networks that are unsecured provide an opportunity for hackers to monitor your online activity. Financial information, as well as usernames and passwords, may also be compromised. It's critical to follow security best practices while working remotely.

Work/Life Balance

Employees who work remotely can forget to clock out. When you do not have a true separation between work and homelife, the line can get fuzzy. Employees who blur those lines feel like they are always working, which can lead to burnout.[4]

...Isolation can make you more productive. For others, working in the office allows employees to build important relationships...



10 Security **Best Practices**

01 Update & Review Policies

It's critical that the following policies are reviewed and are current before allowing users to work from home.

- Remote Working/Telecommuting Policy
- Remote Access Policy *(for both employees and vendors)*
- BYOD Policy *(if employees are using their own devices)*

Make sure all users read and sign acknowledgements for all applicable policies before you allow them to start working remotely. Prior to working remotely, set clear expectations with employees on productivity, communication, organization, regular check-ins, etc.

Provide your employees with what they need to be successful. For example, if they are used to having two monitors, a keyboard and a mouse in the office, consider providing the same equipment for them while they are remote.

02 Enable for Multifactor or Two Factor Authentication (MFA/2FA)

Enabling MFA/2FA is critical for users accessing email and internet-based applications. Microsoft reports that requiring MFA/2FA prevents 99.9% of data breaches.[5] MFA/2FA creates an additional step that hackers have a tough time overcoming. While it makes it harder for attackers, it does not make it impossible.

Insider Tip: MFA/2FA should especially be turned on for Office 365.

MFA/2FA should also be turned on for any VPN access to your institution's network. This applies for both employees and/or vendors.

03 Avoid Public Wi-FI

Do not use free, open or public Wi-Fi, especially for work - you do not know who is listening. If you do not have another option and need to use open/public Wi-Fi, optain a VPN or tether with a mobile device. You can also purchase a wireless hotspot from a cellular provider.

04 Centralize as Much as Possible

Simply stated, keep work on work devices. Make it a best practice that family access is not allowed on work devices. If you have a BYOD (bring your own device) situation, make it an expectation that the device is only used for work while being allowed to work remotely.

SBS Institute[6] recommends Office 365 as an excellent, cloud-based productivity boost. Workers can access anything, including emails and files, from anywhere at any time, all while boasting robust security features. Office 365 also offers a variety of safe, online collaboration tools.

If you have to host applications centrally, do so virtually or on the cloud. For a central location, allow employees to use a VPN to access applications. Do not install them on the actual device unless absolutely necessary.

Make sure patches and updates are distributed centrally. Don't rely on the user to install patches or security updates. Security should also be pushed to the host. End-users aren't security people and shouldn't be relied on to perform security functions.

WI-FI Security

The last thing you want is for someone to access your network or server from their own connection without the proper layer of security.

05 • Protect User Endpoint

The device(s) users access while working remotely (laptops, desktops, smartphones, tablets, etc.) need to be protected against cyberattacks. If workers are using their own devices while working from home, you'll need to either provide them with a license or reimburse them for reputable endpoint security software.

Endpoint Security Solutions

These endpoint security solutions offer an additional layer of security on a device, which is where an attack is most likely to occur.

- Anti-malware
- Email filtering
- Web filtering
- Host-based firewall
- Host-based IDS/IPS
- Encryption
- USB blocking

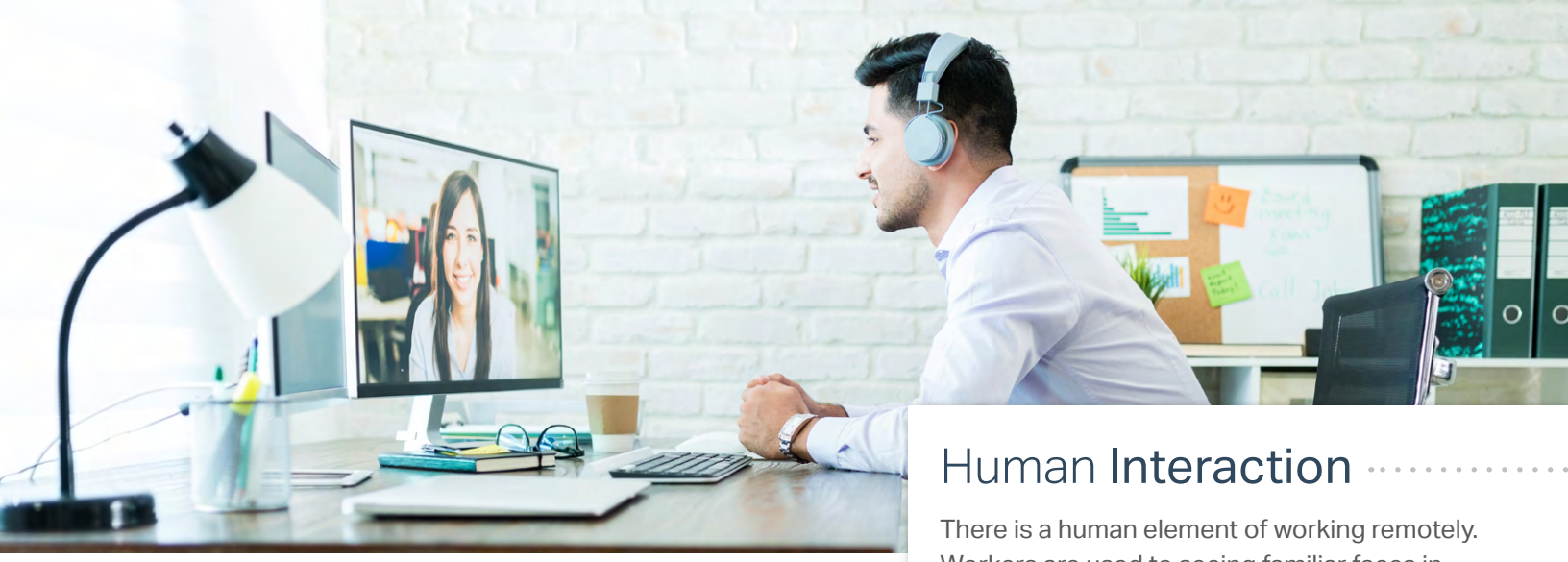
06 • Use Encryption Everywhere Possible

It's best practice to consider encryption everywhere possible. Encryption is the process of encoding data in such a way that only authorized parties can access such information, and those who are not authorized cannot.[7] Use VPN access, not Remote Desk Protocol (RDP). RDP has many known vulnerabilities and is being actively exploited by attackers around the world right now. Additionally, VPN connections provide good encryption, while RDP does not.

Encrypt mobile devices, including laptops and smartphones with full-disk encryption. An example of full-disk encryption is BitLocker. However, there many other solutions on the market.

Ensure both cloud and local storage is encrypted. Email should be encrypted as well. When everyone is working in the office, on the same network, it's not as critical to encrypt email as when you have remote workers sending emails over the internet.

Insider Tip: If you use Office 365, they offer easy instructions to ensure your email encryption is in place.



Human Interaction

There is a human element of working remotely. Workers are used to seeing familiar faces in the office and having human interaction.

07 Use Video Conferencing

If available, using video conferencing can keep people engaged and connected. Using video adds a personal, human touch to remote meetings.

Solutions

These solutions allow your team and individuals to schedule regular check-ins and increase communication.

- Microsoft Teams
- Slack
- Zoom / RingCentral

Insider Tip: Be mindful in knowing your own and your user's bandwidth. If you live in a remote area that does not have fast internet, video conferencing might not be feasible.

08 Know What Your Users Are Doing

Monitor your logs - VPN logs (user and vendor), email logs, user access and activity logs.

Insider Tip: If you use Office 365, enable audit logging in the Security & Compliance Center (SCC).

Restrict access to your network and internet-based applications (like Office 365) by device or country. Blocking network or application access from other locations (such as foregin contries) or devices, prevents hackers from trying to log in from unauthorized locations and devices.

You should also consider investing in a Security Information Event Manager (SIEM). A SIEM is a log aggregator that will give insight into your network and help you to drill down into the million of logs you'll get each day.

Make sure you are communicating with your remote users to understand their workflow. With the right technology in place, it's possible to get daily or weekly summary reports from remote workers. This is a good precaution, especially for those who have never worked remotely before.

09 Segment Networks

Don't just trust everything connected to your network - internally and at home users. Not all devices need to talk to one another; therefore, networks can be segmented. You can use Access Control Lists (ACLs) and Virtual LANs (VLANs) to separate those things that don't necessarily need to talk to one another on your network.

Encourage home users to set up different networks for work-use vs. home-use if they are capable of doing so. Perhaps this could be a guest network and a regular network. Remember, if you are letting someone work from home and you give them access to your network, their home network is now part of your network. Their smart TV and children's tablets don't need acces to your network and should be connected to a separate network.

10 Train Your Remote Workers

Educate your employees about remote working expectations. Let them know what you expect from them and what they can expect from you.

Some employees might need additional training on new tools needed to work remotely. Wheather it's logging into a VPN or using a video conferencing tool, providing your employees with proper instruction will ensure their productivity and success while working remote.

Lastly, ensure your employees are educated on additional cybersecurity threats related to remote work. Hackers prey on fear, and if we are in a situation where employees are forced to work from home, there is bound to be societal fear. Now is the time to be more cyber-vigilant than ever!

References

1. A 2-Year Stanford Study Shows the Astonishing Productivity Boost of Working From Home
   www.inc.com/scott-mautz/a-2-year-stanford-study-shows-astonishing-productivity-boost-of-working-from-home.html

2. Productivity, Retention and Cost Savings: Why Working From Home Benefits Employees And Employers
   www.wbur.org/hereandnow/2019/07/23/work-from-home-benefits

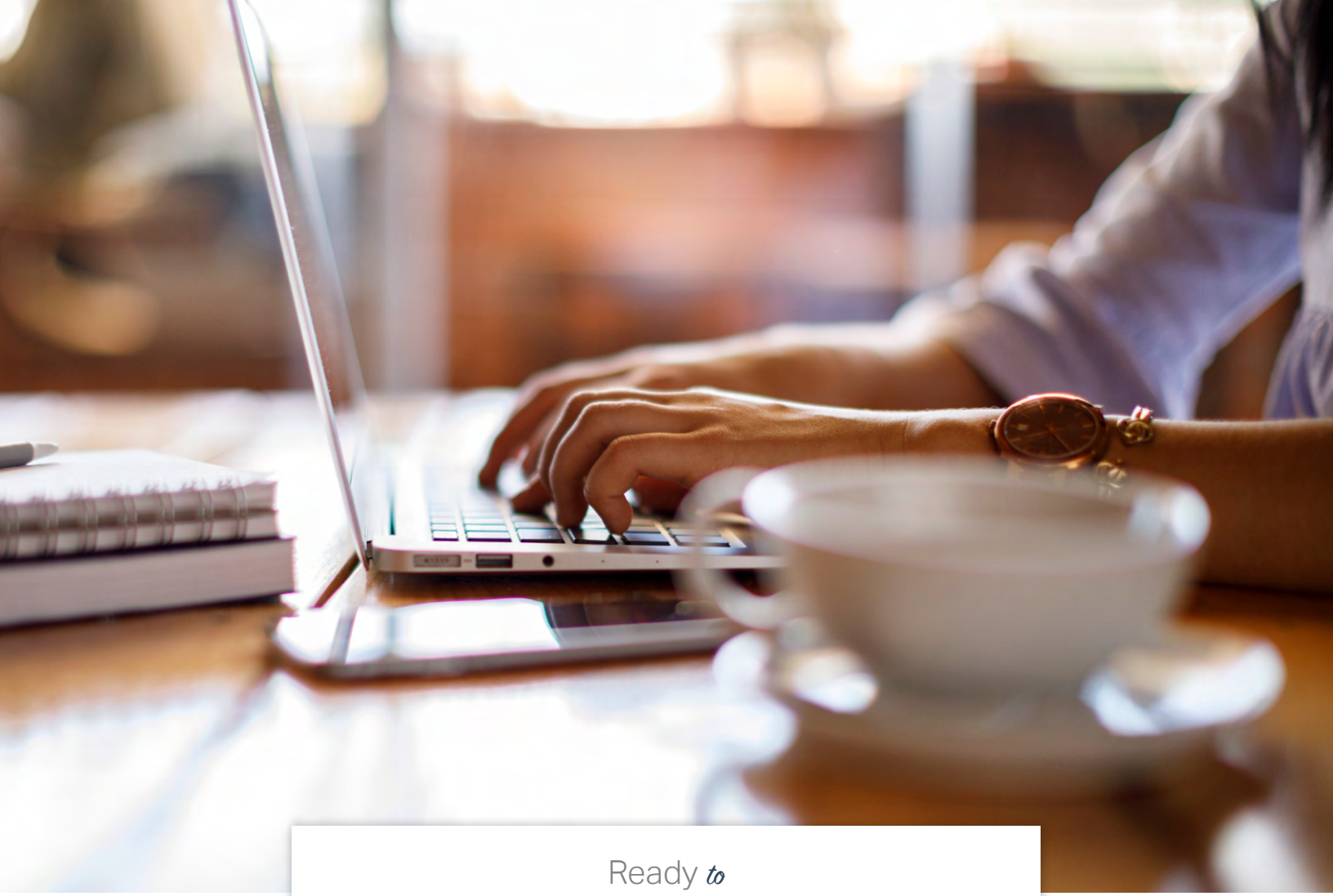
3. 2019 Remote IT Workers Stats: 10 Facts Companies Should Know
   www.tecla.io/blog/2019-remote-it-workers-stats-companies-should-know/

4. Want to work from home? Understand the Pros and Cons Before Deciding
   www.monster.com/career-advice/article/pros-cons-of-working-from-home

5. One Simple Action You Can Take to Prevent 99.9 Percent of Attacks on Your Accounts
   www.microsoft.com/security/blog/2019/08/20/one-simple-action-you-can-take-to-prevent-99-9-percent-of-account-attacks/

6. {Hacking Hour} Understanding Office 365 Security
   www.sbscyber.com/resources/hacker-hour-understanding-office-365-security

7. Encryption - Webster Definition
   www.merriam-webster.com/dictionary/encryption



Ready *to*

WORK REMOTELY?

OnCourse Learning provides a comprehensive solution for your compliance training and personal development needs.

Learn more at OnCourseLearning.com

OnCourse Learning is a member of the Adtalem Global Education Financial Services Workforce Solutions family which includes: the Association of Certified Anti-Money Laundering Specialists (ACAMS), its CAMS certification is one of the most widely recognized anti-money laundering certifications among compliance professionals worldwide; Becker Professional Education, which offers programs in CPA Exam Review and continuing professional education courses; and EduPristine, one of India's leading training providers in accounting, finance and digital marketing.

OnCourse Learning

CONTACT US

Contact OnCourse Learning for more information.

(866) 806 - 9900

www.OnCourseLearning.com