Security for All Things Hybrid: Tips and Tricks to Stay Safe

Underwritten by Fortinet

Introduction

If this was your first experience with virtual private networks, teleconferencing and shrieking kids disrupting meetings, welcome to the new digital age. The pandemic didn't invent a digital world, but only accelerated changes that were already happening in government. Many agencies had designated telework as a priority, but most networks weren't nearly robust or flexible enough to support a jumble of traffic from residences, coffee shops, headquarters and branch offices.

Ta-da. IT and security teams worked their magic, managing to set up and secure widespread connections so that whole populations can work from home. Now, they have that ability up their sleeves.

As vaccines roll out and businesses reopen, cookouts and water coolers all suggest the question: "Are you back in the office?"

More than likely, yours won't be a simple yes or no answer. There will be qualifiers. There will be uncertainty. There will be hybrids.

Your own cyber hygiene, whether you can stay safe without the watchful eyes of security, plays a part in determining where you'll be working, and how much freedom you'll have.

Long-term hybrid and remote work will only be available if your agency can ensure it's secure. Through a series of interactive activities in the following pages, we'll explore what security looks like in the age of hybrid, with personal security tips for home, the office and everywhere in between.

Physical Security in the Digital Era

Government during the pandemic has transcended into the digital world. So thankfully, we really don't have to follow the same in-office safety protocols anymore, right? Actually, wrong.

In our new remote/hybrid state of work, physical security still matters – maybe more than before. Webcams and shared devices put your personal and work information in reach of outsiders. And as home and work lives blend, you're now the keymaster for your own privacy.

To test your knowledge, take this quiz on connecting from afar!

Quiz

Answers are on the following page. Source: FTC

1. Promoting physical securing includes protecting ...

A. Only paper files
B. Only paper files and any computer on which you store electronic copies of those files
C. Only paper files, flash drives and point-of-sale devices
D. All the above, plus any other device with sensitive information on it

2. True or false: Paper files that have sensitive information should be disposed of in a locked trash bin immediately.

3. True or false: When you hit the "delete" key, that means a file is automatically removed from your computer.

4. True or false: Only people with access to sensitive data need to be trained on the importance of the physical security of files and equipment.

5. True or false: Keeping your router's default name will help security professionals identify it and, thus, help protect your network's security.

6. True or false: Before connecting remotely to the agency network, your personal device should meet the same security requirements as agency-issued devices.

7. Which of the following describes the best way to make sure you are securely accessing the agency network remotely?

A. Read your agency's cybersecurity policies thoroughly
B. Use VPN when connecting remotely to the agency network
C. Use unique, complex network passwords and avoid unattended, open workstations
D. All of the above

Answer Key

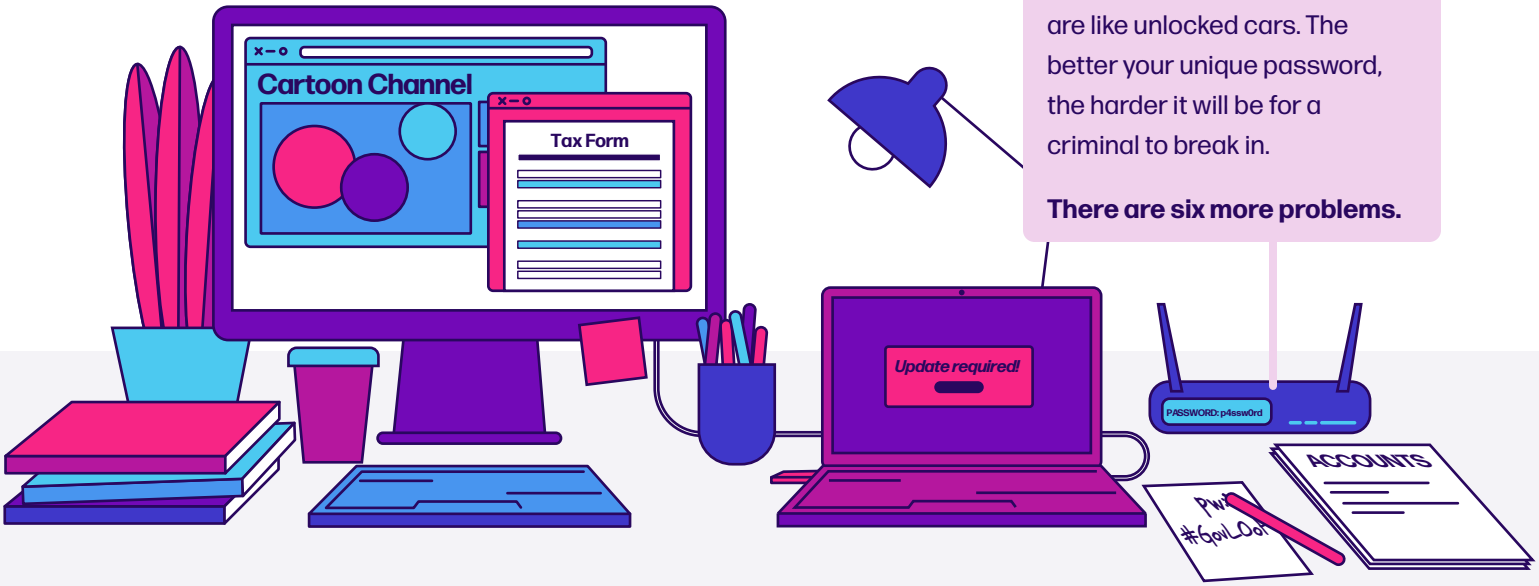
1. **D.** Promoting physical security includes protecting sensitive information in paper files and on hard drives, flash drives, laptops, point-of-sale devices and other equipment.
2. **False.** Always shred documents with sensitive information before throwing them away.
3. **False.** "Delete" alone does not actually remove a file from a computer. Use designated software to erase data, especially before you donate or discard old computers, mobile devices, digital copiers and drives.
4. **False.** Everyone needs to have strong physical security practices, and everyone should also be trained on what to do if equipment or paper files are lost or stolen, including whom to notify and what to do next. You can find more at FTC.gov/DataBreach.
5. **False.** Changing your router's default name and preset password can help protect your router from hackers.
6. **True.** When connecting remotely to the agency network, your device should meet the same security requirements as agency-issued devices that connect directly to the network.
7. **D.** Secure remote access requires all of these steps.

What's Wrong With This Image?

Something's going on here. Can you spot what's wrong?

Here's a freebie:
Change the default password on your home router. Cybercriminals are like car thieves, and default passwords are like unlocked cars. The better your unique password, the harder it will be for a criminal to break in.

There are six more problems.



Answers are on Page 7.

Security for Government, Everywhere You Need It

Federal, state, and local governments face rising cyber threats, tenuous budget forecasts, and the continuation of remote work.

Fortinet has the solutions agencies need to:

- Protect digital assets and critical infrastructure against advanced attacks
- Make the most of limited spending power
- Take advantage of key support programs and opportunities available from the Cares Act and the American Rescue Plan

INDUSTRY SPOTLIGHT

Telework Demands Secure Connections

An interview with Jim Richberg, CISO, Public Sector, Fortinet

Timing is everything. Imagine a global pandemic 10 years ago. Even then, such widespread telework wouldn't have been nearly as possible. And 20 years ago? Forget about it.

The move to large-scale remote work wasn't just about getting laptops to households. Rather, by 2020, network size, speed and availability had matured to a point where agencies – including some of the nation's largest employers – could reliably support their employees using wireless connections to reach the network. That left security playing catch-up.

"Serendipity played a role in success at doing remote telework — where many agencies were in their upgrade cycle and what technology choices they had made," said Jim Richberg, Chief Information Security Officer for Public Sector at Fortinet, a network security provider.

Agencies have succeeded thus far, but a digital world demands even more advanced network security structures. To progress, agencies can follow the below steps.

1. Recognize new patterns of work

2020 was "the year of the hybrid," Richberg said.

The move to telework — portending shifts to longer-term hybrid environments — bore fascinating patterns, from shared school and work computer stations to work hours expanding beyond 9 to 5. These trends meant security teams had to re-evaluate red flags. Late-night logins and unrecognized activity used to be indicators of a breach; now, they blend into the work-life puree of every employee.

Another trend of note: Agencies everywhere opened up previously in-person jobs to geographically distant employees. Since employees didn't need to be office-bound, employers sourced from a broader pool of candidates. This was a major win for hiring teams, but blurred the important filter of location for network security administrators, who previously marked an activity as suspicious if from an unrecognized location.

2. Understand faces on networks

Out-of-state employees aren't the only fresh faces on networks. Agencies have turned to robotic process automation – which has its own access credentials – to help handle the surge of citizen requests and resolve backloads.

Security teams now must authorize and secure large numbers of connections to disparate internal databases. And as the digital surface grows, the threat landscape does too. Multi-vector, multi-impact, mixed "best of breed" attacks and AI-assisted targeting are becoming more commonplace.

Differentiating between legitimate and malicious network traffic will remain a challenge.

3. Roll out SD-WAN

Agencies can embrace the remote revolution by adopting a software-defined wide-area network (SD-WAN). SD-WAN reduces the cost and burden of providing remote workers with access to applications and data. And since security controls are integrated at the edge, traffic doesn't need to travel back to the data center, boosting the user experience.

Integrated security also improves visibility, helping administrators cut through the tangle of devices, accounts and profiles that clog up modern networks. Fortinet SD-WAN solutions also use automation to make connections simpler.

"The key should be spending smarter," Richberg said. "And a key for governments is doubling down on upgrades such as SD-WAN, which saves money, increases staff efficiency, both IT and security, improves the user experience, and enhances security, productivity and resilience."

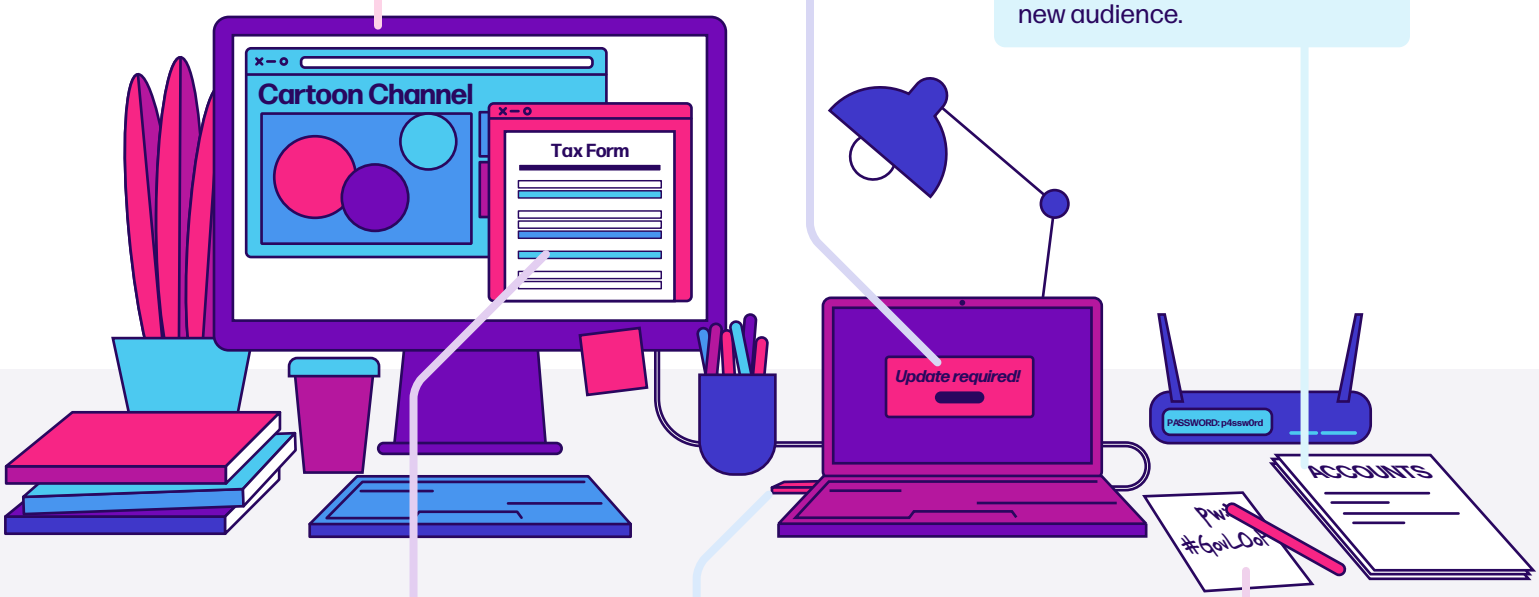
What's Wrong With This Image?

Answers and tips for your at-home environment

Turn off or sleep your computer as soon as you're away from it. Even if you're at home, a house member or guest could see and use the information or accidentally share or capture it.

Set up auto updates to keep your computer's security software up to standard. Doing so means you'll receive patches to vulnerabilities as soon as they're available. If it's your work laptop, please ask your IT department first. They might want you to wait until they can vet the latest update.

Clear your desk of sensitive information. Even if no one in your immediate household poses a risk, webcams can bring your home life to a whole new audience.



Limit access to sensitive personal and work documents on your computer to just yourself. If you're relying on a personal device that the family has to use, make sure you connect securely, have antivirus protections and spam blockers, and close out all programs once done with them. You can even consider creating a separate computer account for work.

Double-check that this device is agency-approved. Otherwise, it should be nowhere near your laptop. Hackers can use flash drives and disks to install malware on your devices.

Never write down your passwords on paper. Rely on ones that you can keep in your head, or use a password manager instead.

Note: Install software and firmware updates on your router as soon as possible.

Cybercriminals are constantly looking for ways to take advantage of vulnerabilities (unsecure or weak programming) in your router. By updating your hardware as soon as new releases are available, you ensure you're one step ahead of villainy.

Summary: Secure Your Remote Workstation

- ✓ Use a strong password for your workstation and never share it. A strong passphrase (two or more words + numbers + symbols) is easy to remember but hard for a criminal to guess or crack. **If you have too many passwords to remember, try using a password vault. Not only can those store all your passwords, but password managers even create unique ones so you don't have to.**
- ✓ Just like with your router, **make sure you are updating your computer's operating system and computer hardware.** The newer versions of Apple and Windows offer automatic updates, giving you one less thing to keep on your to-do list.
- ✓ **Use multifactor authentication or two-factor authentication (2FA) everywhere it is offered.** Most banking apps and email providers offer one of these options, making sure that even if that super-secret password gets lost or stolen, the thief can't get to your sensitive information. For the best security, use an MFA/2FA app instead of text messaging or voice calling.
- ✓ **Lock before you walk.** The information on your workstation is for your eyes only. If you are using a personal computer for work, set it to auto-lock to ensure it will lock automatically if you forget to do it yourself before you walk away.
- ✓ You're not the only one who can get sick from a virus. **Your computer is at high risk of getting infected unless you use an antivirus program and keep it up to date.**
- ✓ If you are working with sensitive data that is covered by local or federal privacy laws, **make sure nobody else can see your screen or overhear your conversations.**
- ✓ **Turn on device encryption for your personal computer** to ensure that, if it gets stolen, nobody else can get to your sensitive information. MacOS users can turn on FileVault and Windows users can turn on BitLocker; both are available for free on newer versions.
- ✓ **Keep work life and personal life separate on your laptop.** Do not store work information on personal devices and vice versa. If at all possible, obtain a government-issued device to work from home. If one is not available, ensure your personal device is set up similar to how your work one is. Ask your tech support team for help.
- ✓ **Back up your important information.** If you are using a government-issued device, make sure you are saving all your work on a network folder or in a work-approved cloud storage area. If you are using a personal device, back up your personal information using a secure, password-protected cloud storage service (like Azure, Google Cloud, DropBox or others).
- ✓ Avoid using public Wi-Fi, but if you need to use it, **use a VPN connection** to prevent criminals from intercepting your internet traffic and stealing your information.

Source: Maricopa County

Just remember: PLUMBERS!

Wait, what?

PLUMBERS!

Password-protect accounts and devices
Lock your workstation and screen
Update operating systems
Multifactor-authenticate your accounts and info
Back up your info
Encrypt your personal computer
Report any attacks
Separate work and home lives

Next Steps

Cybersecurity isn't a one-trick pony. The tips and tricks outlined in these few pages are only small parts of securing a hybrid work environment.

The other factors can be found in "Your Cybersecurity Handbook: Tips and Tricks to Stay Safe." There, you'll explore the other parts, and we walk you through with fun activities, games and even a crossword puzzle.

govloop

1152 15th St. NW Suite 800
Washington, DC 20005

P: (202) 407-7421 | F: (202) 407-7501

www.govloop.com
@GovLoop