Cybersecurity Kit:

4 Proven Cybersecurity Tips for Telecommuters

Cybercriminals are con men and women in disguise who constantly look for opportunities to get their hands on your sensitive data, or even your funds. Employees who work remotely, whether full time or occasionally, can represent easy targets outside the cyber-safe confines of your offices. This Cybersecurity Kit shares basic tips that will help your employees make cybersecurity a priority whenever and wherever they do their jobs.

How to use this training resource

1. Print the attendance roster, and ask employees to sign it. Keep the roster with your employee training records.
2. Give each employee a copy of 4 Proven Cybersecurity Tips for Telecommuters.
3. Use the talking points in the instructor notes to walk through the training. The notes include engagement opportunities that transform the material from words on a page to practical tips for staying safe on the job.
4. When you are finished walking through the material, ask employees to take the quiz.
5. Score the quiz using the answer key. Keep copies in your employee training records, and plan follow-up training based on quiz results.

Attendance Roster

Date of training: _____

Location:_____

Conducted by: _____

Topics covered:

- Secure your device
- Protect sensitive data
- Escape prying eyes – and ears
- Keep unwanted visitors out of virtual meetings

Name	Signature	Department	School/Location

Name	Signature	Department	School/Location

4 Proven Cybersecurity Tips for Telecommuters

Working remotely has advantages. You get to dress comfortably, spend the day wherever you're most productive, and steer clear of rush hour traffic. But with perks come risks. When you work outside the office, you could unintentionally open doors for cybercriminals. Remember that you are responsible for the security of your device and the data it holds.

Tip 1: Secure your device

- ✓ Don't store it in your vehicle.
- ✓ Implement a hands-off policy for family and friends
- ✓ Keep it with you in public if possible
- ✓ Report missing devices immediately

Tip 2: Protect sensitive data

- ✓ Avoid unsecured Wi-Fi
- ✓ Log in through the virtual private network (VPN)
- ✓ Watch out for imposters
- ✓ Use secure file-sharing platforms
- ✓ Don't put sensitive information on portable devices
- ✓ Steer clear of flash drives

Tip 3: Escape prying eyes – and ears

- ✓ Be careful what you throw away
- ✓ Watch for shoulder surfers
- ✓ Step outside for confidential conversations
- ✓ Lock your screen

Tip 4. Keep unwanted visitors out of virtual meetings

- ✓ Require a meeting password
- ✓ Create a unique meeting ID
- ✓ Lock your meetings
- ✓ Allow invited visitors only

If the meeting must be public

- ✓ Use the waiting room
- ✓ Lock down screen and audio controls
- ✓ Restrict certain file types

Instructor Notes

Working remotely has advantages. You get to dress comfortably, spend the day wherever you're most productive, and steer clear of rush hour traffic. But with perks come risks. When you work outside the secure confines of the office, you could unintentionally open doors for cybercriminals. Remember that you are responsible for the security of your device and the data it holds. Today, you will learn how to do your part to protect the organization against cybercrime.

Agenda

- Secure your device
- Protect sensitive information
- Escape prying eyes – and ears
- Keep unwanted visitors out of virtual meetings

Secure your device

Our information technology department set up your employer-issued laptop or mobile device to be as secure as possible. Always use it, not a personal device, to conduct work-related business – and vice versa. Taking your device home or on a business trip carries risks.

Tips	Instructor talking points
Don't store your device in your vehicle	If you can't avoid it, lock it in the trunk if you have one. If not, store it somewhere out of sight. Remember that extreme temperatures can damage the device if you leave it in a vehicle too long.
Implement a hands-off policy	The policy should apply to everyone in the home. Children are digital natives who know their way around the internet. They could visit malicious websites or install harmful apps or software.
Keep it with you in public spaces if possible	When traveling or working in a public space, do not leave your device unattended. If you're staying in a hotel, take it with you when you leave if possible. If you can't, lock it in your room safe or the hotel safe, but make sure it is fully powered down.
Report missing devices immediately	Notify IT if your device is lost or stolen. They might be able to erase the data remotely.

Protect sensitive data

Think about all the birthdates, addresses, payroll information, and even health records we maintain on students, staff, and parents. It's all personally identifiable information cybercriminals can sell on the Dark Web.

Tips	Instructor talking points
Avoid unsecured Wi-Fi	Your favorite coffee shop might seem like the ideal place to relax and dig into your work. Unfortunately, most public Wi-Fi options are unsecured. Similarly, you should avoid hopping on your neighbor's Wi-Fi if yours is unavailable. Logging in through your own password-protected Wi-Fi is one of the most secure ways to work remotely. **Note to presenter: If your organization offers secure mobile hotspots to employees, consider mentioning it here.**
Log in through the virtual private network (VPN)	A VPN is a secured gateway into our network. Everyone is required to use the VPN when logging into the network remotely (See engagement opportunity below). **Note to presenter: Your VPN's multi-factor authentication should be turned on.**
Watch out for imposters	Hackers might try their luck at impersonating IT department staff. In this scenario, you could receive a call like, "Hey, we noticed you were having some trouble with your VPN. Could you give us your username and password?" Tech support will not likely reach out to you unsolicited. Familiarize yourself with what official communication looks like from our IT team, and stay vigilant.
Use secure file-sharing platforms	If you need to exchange sensitive information with co-workers, use the organization's shared drives. You might also be authorized to use a file-sharing platform such as Dropbox, OneDrive, or a Google Drive. If so, confirm that the platform is encrypted before sharing sensitive data. Additionally, you might be able to use an in-company File Transfer Protocol program (FTP), which allows for encrypted transfer of data. Talk with the IT team to identify the best method for secure transfer of sensitive files.

Don’t put sensitive information on portable devices	Portable devices are easy to lose or steal. Leave confidential information in the office, or access it remotely through VPN.
Be careful with flash drives	It might be more convenient to store a project on a flash drive and take it home than it is to go through VPN. Like portable devices, however, flash drives can be lost or stolen. If you use a flash drive, choose the encrypted variety or, at minimum, password-protect your files.

Engagement opportunity. Show the group how to access and log in through the VPN. Ask them to follow along with you.

Escape prying eyes – and ears

Cybercriminals don't always use malware and other sophisticated technical tools to pull off their scams. Sometimes, they just keep their eyes and ears open.

Tips	Instructor talking points
Be careful what you throw away	Don't throw sensitive work documents in your home trash can. Shred them before you dispose of them.
Watch for shoulder surfers	In cybersecurity circles, shoulder surfing is a scam in which criminals closely watch victims as they enter passwords or work with sensitive content.
Step outside for confidential conversations	You should also avoid using speaker phone in public spaces. You never know who might be listening.
Lock your screen	Rentable coworking spaces are popular among freelancers and remote employees. If you use a coworking space and you need to step away, lock your screen so nobody can see it.

Keep unwanted visitors out of virtual meetings

Software platforms such as Zoom, GotoMeeting, Cisco WebEx, and Skype empower us to connect with our colleagues remotely, but they also carry vulnerabilities. Cybercriminals might take advantage by hijacking meetings in an action known as "zoom-bombing."

Tips	Instructor talking points
Require a meeting password	Only supply the password to designated attendees. This will reduce the risk of an unwanted visitor disrupting your meeting.
Create a unique meeting ID	Only those who have the meeting ID can access the event. Meetings IDs, combined with password protection, will go a long way in defending your meeting from malicious activity.
Lock your meetings	Once your attendees have joined and your meeting has started, you can lock the room so no new attendees have access.

Allow invited visitors only	You can set your meeting to only allow invited visitors to attend. If you do not use this security feature, invited visitors could forward the meeting information to others.
If the meeting must be public	
Use the waiting room	The waiting room option allows you to verify that potential attendees are known and expected collaborators. Any unknown visitors can be left in the waiting room until verified.
Lock down screen and audio controls	The meeting organizer should be able to control who can display their screen during the meeting. They will also have control over who can broadcast to the group with their webcam or microphone.
Restrict certain file types	Malicious actors have inserted offensive, animated .gif files into Zoom meetings. Organizers can restrict which file types are allowed in the meeting.

Employee Quiz

1. It's okay to let your family use your employer-issued laptop as long as you explain that they should not download software or apps.
   - True
   - False
2. What should you do with your laptop if you're traveling and you can't take it with you when you leave your hotel room?
   a) Hide it under the bed
   b) Leave it in your luggage
   c) Lock it in your room safe or the hotel safe
   d) Lock it in your room
3. Why should you avoid using public Wi-Fi?
   a) It's too slow
   b) It's typically unsecured
   c) Many websites are blocked
   d) You have to share sensitive information to access it
4. It is common for our IT staff to reach out to employees unsolicited and ask for their username and password.
   - True
   - False
5. The most secure way to use a flash drive is to:
   a) Make sure it is encrypted
   b) Keep it in your laptop bag when you're not using it
   c) Encrypt the files you save on the flash drive
   d) Keep it away from magnets, which could erase your data
6. You are required to log in through VPN when working remotely.
   - True
   - False

7. What should you do with hard-copy, sensitive documents when you need to dispose of them while working remotely?
   a) Burn them
   b) Put them in your recycling bin
   c) Shred them
   d) Put them in your trash can
8. You should avoid saving sensitive information on portable devices such as tablets.
   - True
   - False
9. If a meeting must be public, you should (Choose all the apply):
   a) Use the waiting room
   b) Create a unique meeting ID
   c) Restrict screen and audio controls
   d) Lock the meeting
10. Most virtual collaboration tools allow you to set your meeting so only invited guests can attend
    - True
    - False

Employee Quiz Answer Key

1. It's okay to let your family use your employer-issued laptop as long as you explain that they should not download software or apps.
   - True
   - False

   Correct answer: False

2. What should you do with your laptop if you're traveling and you can't take it with you when you leave your hotel room?
   a) Hide it under the bed
   b) Leave it in your luggage
   c) Lock it in your room safe or the hotel safe

   Correct answer: c

3. Why should you avoid using public Wi-Fi?
   a) It's too slow
   b) It's typically unsecured
   c) Many websites are blocked
   d) You have to share sensitive information to access it

   Correct answer: b

4. It is common for our IT staff to reach out to employees unsolicited and ask for their username and password.
   - True
   - False

   Correct answer: False

5. The most secure way to use a flash drive is to:
   a) Make sure it is encrypted
   b) Keep it in your laptop bag when you're not using it
   c) Encrypt the files you save on the flash drive
   d) Keep it away from magnets, which could erase your data

   Correct answer: a

6. You are required to log in through VPN when working remotely.
    - True
    - False

    Correct answer: True

7. What should you do with hard-copy, sensitive documents when you need to dispose of them while working remotely?
    a) Burn them
    b) Put them in your recycling bin
    c) Shred them
    d) Put them in your trash can

    Correct answer: c

8. You should avoid saving sensitive information on portable devices such as tablets.
    - True
    - False

    Correct answer: True

9. If a meeting must be public, you should (Choose all the apply):
    a) Use the waiting room
    b) Create a unique meeting ID
    c) Restrict screen and audio controls
    d) Lock the meeting

    Correct answer: a, c

10. Most virtual collaboration tools allow you to set your meeting so only invited guests can attend
    - True
    - False

    Correct answer: True