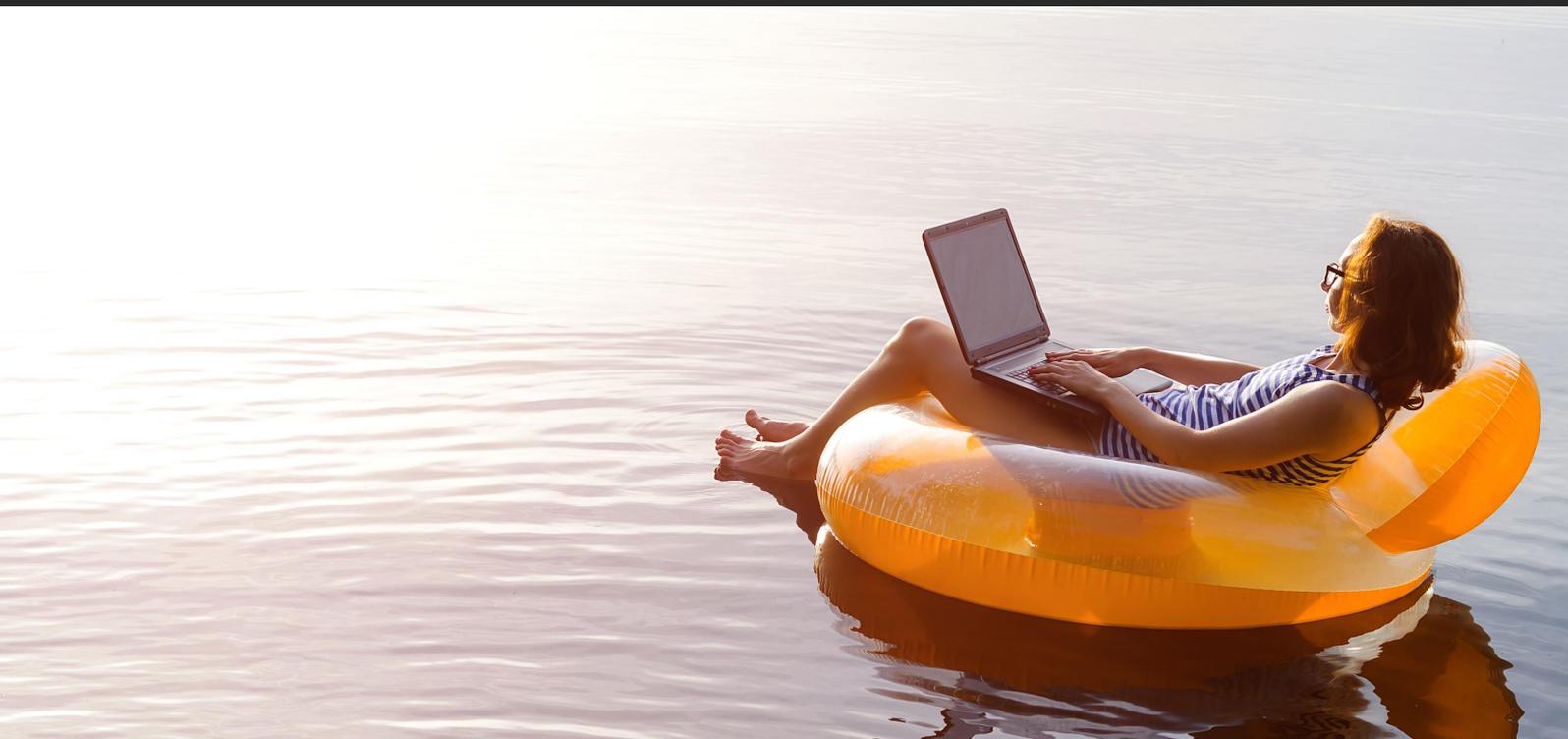


REMOTE ACCESS SECURITY

A review of the latest security threats and how you can avoid them



THIS MONTH'S TOPICS:

Secure Transportation
- pg. 2

Optimizing your WFH experience - pg. 3

Scam of the Month - pg.4

Key Takeaways - pg. 5

"The new normal." We've been hearing that term a lot lately. Now, this term may not be reflect everything we are currently experiencing, but the dramatic pivot to work from home (WFH) may have a lasting impact.

WFH has been crucial in keeping employee health and safety a top priority in uncertain times. During that bridge, many organizations and employees have seen the benefits in a remote work environment and glimpses of a largely remote workforce are beginning to take shape at some businesses.

With this push to remote work, it is crucial that workforce members are prepared in how to handle a WFH lifestyle securely and while retaining some sanity.

Secure Transportation

Taking our work home has become a new way of life for many of us. Transporting equipment or paperwork may seem simple, but there are many security precautions to consider before embarking on your quest.



Get approval from your supervisor before taking anything out of the office. Keep a list of what you are taking out and when for your reference.



Avoid making any unnecessary pit stops when traveling with sensitive data. Leaving devices unattended could leave them vulnerable to theft.



When you're ready to transport, make sure you are physically securing and locking devices. Keep them locked in the trunk of your car if you can!



When you do make it to your final destination, continue maintaining physical security, and keep devices locked whenever possible.

Key Takeaways

Criminals don't need any sophisticated skills like hacking or social engineering to steal a device from a vehicle.

Talk Nerdy to Me! with Brainiac Bill



Encryption

The best defense against theft is to have your device encrypted. Encryption won't prevent your device from being stolen, but it will protect the data residing on the device's hard drive from unauthorized access. Any data on an unencrypted device that is stolen would be considered accessible to the thief, resulting in a breach.

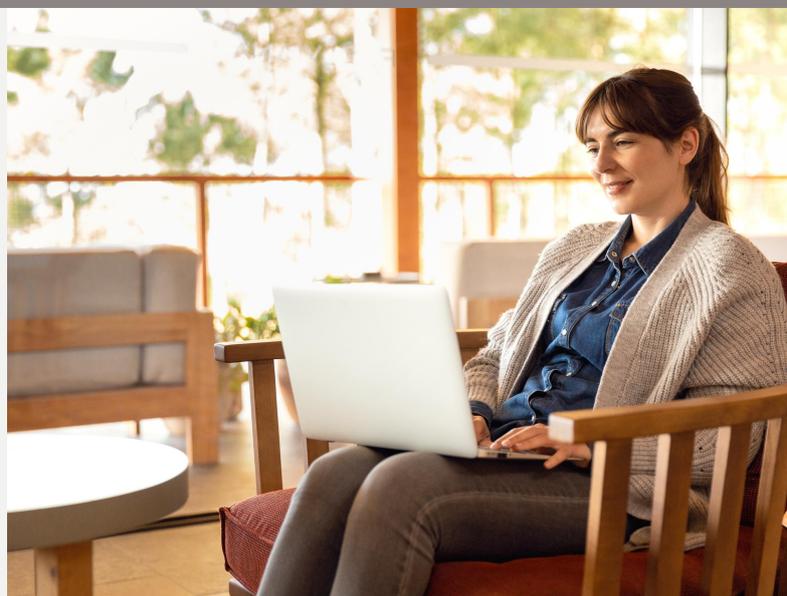
OPTIMIZING YOUR WFH EXPERIENCE

Working from home has been a major adjustment for many. Quite frankly, some love it and some don't. No matter what side you're on, here are some non-technical tips for working remotely.



- ✓ Create a dedicated workspace where you can focus on performing your tasks.
- ✓ Stick to your normal working hours, performing work-related tasks during the workday, and save home tasks for after working hours.

- ✓ Find a space with natural light or spend some time during your day outside.
- ✓ Socialize responsibly. Try communicating with your coworkers through office tools set up by your company.



- ✗ Minimize distractions as much as possible during your workday.
- ✗ Avoid turning on the television, playing games, or browsing the web. It can wait until your break or after the workday is done.

SCAM OF THE MONTH

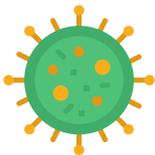
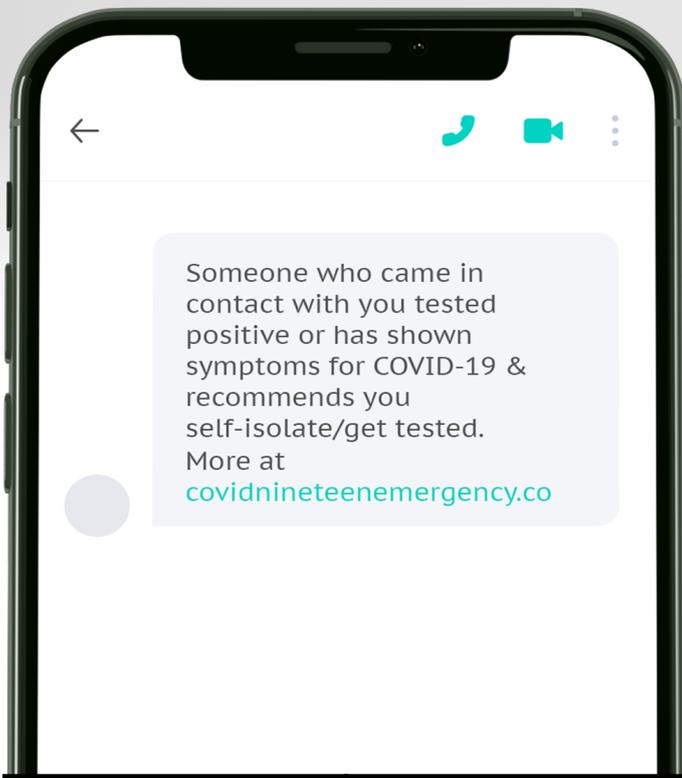
Each month we highlight a REAL scam that was submitted to our security team. We highlight these real examples of tactics criminals are using RIGHT NOW, that way you'll be better prepared when the next scam comes your way.

This month's submission comes from "Cindy." Cindy received a text message informing her that she had come into contact with someone testing positive for COVID-19. In the text, she was encouraged to take precautions and click the provided link for more information.



Did you spot the red flags?

- ▶ The text avoids providing any specific information that may help verify its authenticity. But, even if a text does provide details like your name and location, you should still be skeptical.
- ▶ The link is fake and will most likely lead to a malicious web page. Avoid clicking any links in text messages from unknown sources.
- ▶ The text message is using a hot button topic to help initiate activity. This global pandemic is still a prime concern across the globe, so it is very common for criminals to use these popular subjects to peddle their crimes.



Texting scams and others like this have been constant since the global pandemic emerged. Variations of this scam have surfaced and will continue to be updated to better reflect the current trends in our community, Treat unsolicited text messages with extreme caution!



Texting scams are some of the more common scams a criminal can partake in. By using tools or apps, scammers can spoof their phone number and quickly send thousands of fake messages. It all becomes a low risk, high reward option for them, especially with a popular subject matter.



Cindy was wise here and did not click the suspicious link and did not reply to the text. It is best to delete these messages when they come in so that you don't accidentally click something at a later time. Cindy also informed her friends and family too, as this attack can target anyone!

REMOTE WORK IS HERE TO STAY

While all our work may not be remote right now, recent events have made these discussions and options more realistic for safety and business reasons.

Key Takeaways

Grab WFH by the horns and show it how you operate! Taking charge of how your remote work experience is structured is the key to your success!



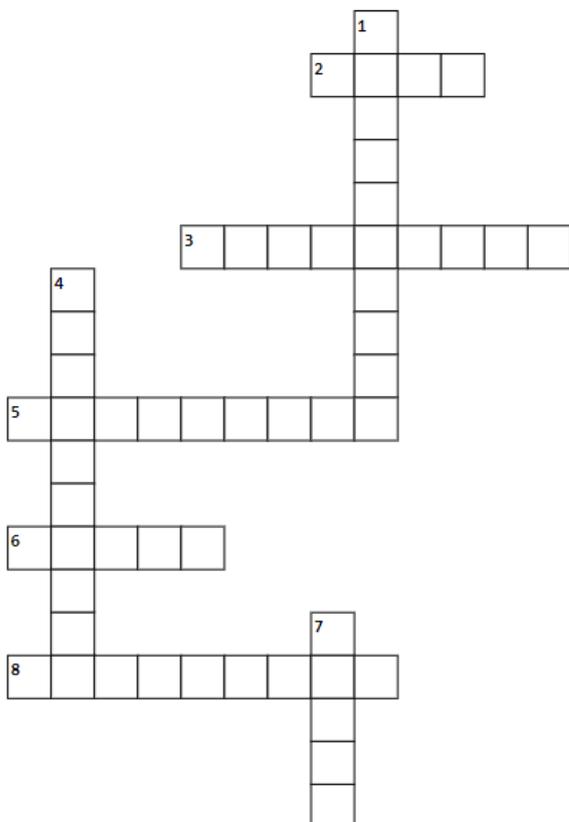
If you must adopt a work from home lifestyle, set yourself up for success by creating a dedicated and comfortable space that is free from distractions.



Keep the physical security of devices as a top priority when taking equipment to and from the office. Minimize pit-stops and protect devices with encryption if possible.



Be on the lookout for any COVID-19 related texting and phishing scams that are currently rampant.



Cybercrime Crossword

Complete this week's activity and find the keywords from this month's newsletter to complete the crossword!

Across

2. A texting scam will try to get you to click this
3. Conversing with coworkers
5. Your workspace should be this; call it your own
6. Person who received the texting scam
8. Taking a device out of the office

Down

1. Watching cartoons at work will make you this
4. Contact this person if you are taking a device out of the office
7. Keep devices and paper files locked up here if you have one