



Inspired eLearning March Newsletter



WEBINAR: CHAT WITH THE FBI

Join Inspired eLearning and the FBI on March 24th at 1:30pm CST for a live discussion on trending cyberthreats and what role the human element plays. Register today!

[REGISTER NOW](#)



SECURITY AWARENESS TIPS POSTERS

Our new security awareness posters are a great way to share cybersecurity best practices with your organization every day.

[DOWNLOAD NOW](#)

5 Tips to Work Safely When Remote

As the coronavirus spreads across the globe, organizations like Apple and Twitter are urging and requiring, employees to work remotely. If your organization is offering you this option, it's important that you continue to keep cybersecurity best practices top of mind. Although you may not be in the office, cyber-criminals can still find their way into your organization's network if you're not careful.

Follow these 5 tips to keep yourself and your organization safe while working remotely:

1) Get prior authorization and instructions before accessing your organization's information when working remotely.

When working remotely from home or while on the road, it's important to take precautions before you access proprietary and sensitive data from your organization. Your Internet connection may not be as secure at home or while you are traveling, giving hackers an opportunity to steal data. Use a

secure VPN connection or follow the instructions provided by your organization.



2) For wireless network connections, be sure to use Wi-Fi Protected Access version 2 (WPA2).

WPA2 provides authentication to allow access for only authorized users and encrypts all data in transit over the wireless connection, securing it from attackers. At home, use WPA2 Personal or WPA2 Home. At work, use WPA2 Enterprise.

This is the strongest authentication and encryption mechanism available and helps to protect your information.

3) When using Wi-Fi in a public place, make sure you connect to the correct Wi-Fi network.

Whenever you're connecting to a new Wi-Fi network, you should ask someone what the correct Wi-Fi name should be. You should never assume based on the name that a Wi-Fi connection is the correct one; anyone can create a Wi-Fi access point under any name designed to collect information. A Wi-Fi network named "CoffeeShopGuests" at a coffee shop may be created by someone who is the street. Once you are connected to a Wi-Fi access point, the data you transmit can become vulnerable.

4) When using Wi-Fi connections, protect yourself by using SSL connections.

Public Wi-Fi connections rarely provide adequate security. The use of a good Virtual Private Network (VPN), like NordVPN can provide a level of security that is better than relying on the security provided by the network. A Secure Sockets Layer (SSL) connection is an encrypted method of connecting to the web. Whenever you connect to sensitive data through a website, you should be using an SSL connection. You can identify a website that is protected by an SSL connection by looking for "<https://>" rather than "<http://>" at the beginning of the URL. An SSL connection will also have a lock icon next to the URL.

5) Always keep mobile devices and laptops with you when working remotely.

When you're out in the field and working remotely, remember to keep a close eye on your smartphone and laptop. Don't leave your device unattended.

For a full list of 10 tips, read the full blog [here](#)

US State Dept. Shares Insider Tips to Fight Insider Threats

Every employee has the potential to become an insider threat, whether through accidental or malicious means. Organizations with the right steps in place can both prevent a person from going rogue and detect these threats before it's too late.

At the US Department of State, everyone who has virtual or physical access to its network, facilities, or information is considered an insider, said Greg Collins, a contractor policy adviser, during an RSA Conference session this week on insider threats. "Anything that they can access and attempt to misuse is an insider threat," Collins explained.



"It is not just a tech problem, it's not just a security issue, and it's not just a personnel issue," added Jackie Atilas, insider threat program director at the State Department. When an

insider threat takes place, businesses can't go back and change what happened, but they can look back and see the indicators that were available to them in order to prevent future threats.

These markers can be spotted at all stages of the employee cycle, Collins said, a process that typically looks the same for organizations across industries and includes the following steps: hiring, vetting, training, inclusion, support, and security. He and Atilas took an insider threat scenario and viewed it through each step to pinpoint red flags indicating malicious activity.

In their example scenario they used an employee who sends an email containing sensitive internal data to someone outside the organization. "This keeps me up at night," Collins said. "This is something you absolutely don't want to happen."

But it does happen, and when it does, it's important to first substitute the individual's name with a unique identifier. "One thing we really stand behind is trying to prevent reputational harm," Collins said. If insider activity has occurred but you don't know if there was malintent, it's best to keep the individual anonymous so as to not muddy the person's name. Once the case has been established, you can start to backtrack and determine where, exactly, they went wrong.

"Managers need to manage; managers need to engage," Atilas said. "Supervisors are the best defense against insider threat behavior. There is a difference between an introverted employee who wants to alone sometimes and an isolationist who exclusively keeps to themselves all day."

This article was originally posted by Dark Reading. Read the full article [here](#)

Coronavirus phishing emails: How to protect against COVID-19 scams

The overwhelming amount of news coverage surrounding the novel coronavirus has created a new danger — phishing attacks looking to exploit public fears about the sometimes-deadly virus.

Cybercriminals send emails claiming to be from legitimate organizations with information about the coronavirus. The email messages might ask you to open an attachment to see the latest statistics. If you click on the attachment or embedded link, you're likely to download malicious software onto your device.

The malware could allow cybercriminals to take control of your computer, log your keystrokes, or access your personal information and financial data, which could lead to identity theft.

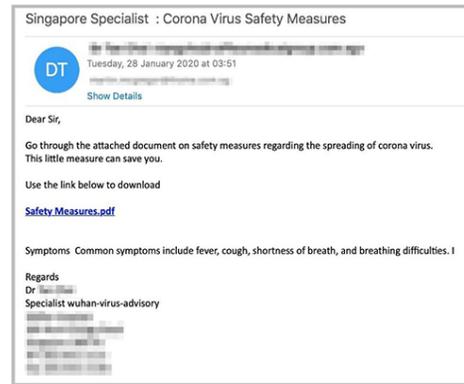
Here are two examples of coronavirus related email scams:

CDC alerts. Cybercriminals have sent phishing emails designed to look like they're from the U.S. Centers for Disease Control. The email might falsely claim to link to a list of coronavirus cases in your area. "You are immediately advised to go through the cases above for safety hazard," the text of one phishing email reads.

Workplace policy emails. Cybercriminals have targeted employees' workplace email accounts. One phishing email begins, "All, Due to the coronavirus outbreak, [company name] is actively taking safety precautions by instituting a Communicable Disease Management Policy." If you click on the fake company policy, you'll download malicious software.

How do I avoid scammers and fake ads?

- Scammers have posted ads that claim to offer treatment or cures for the coronavirus. The ads often try to create a sense of urgency — for instance, “Buy now, limited supply.”
- At least two bad things could happen if you respond to the ads.
- One, you might click on an ad and download malware onto your device.
- Two, you might buy the product and receive something useless, or nothing at all. Meanwhile, you may have shared personal information such as your name, address, and credit card number.
- Bottom line? It’s smart to avoid any ads seeking to capitalize on the coronavirus.



This article was originally posted [here](#).

Product Updates

We have exciting new updates to share! Click below to learn more about what Inspired eLearning is doing to better our product experience for our customers.

LEARN MORE

Connect with us:



© 2020 Inspired eLearning, LLC. All rights reserved.

info@inspiredelearning.com | 800.631.2078

4630 N Loop 1604 W, Suite 401

San Antonio, TX 78249 USA

[Privacy Notice](#)