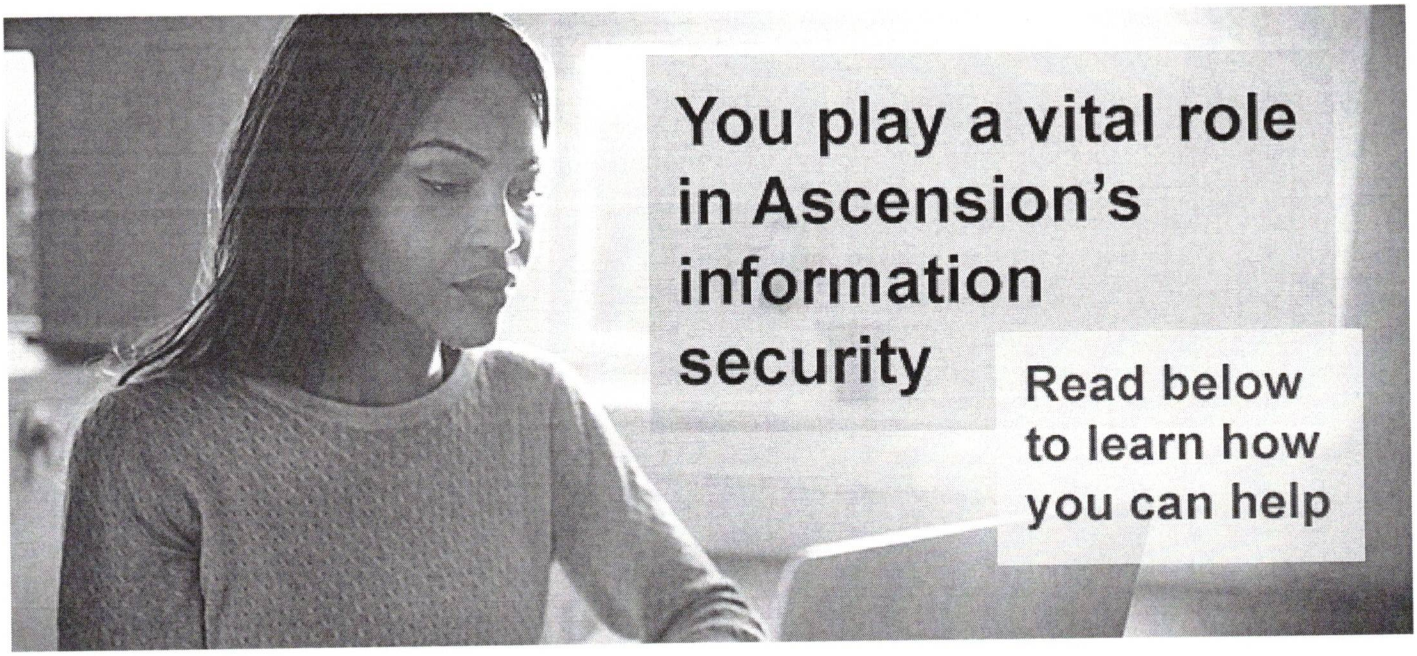
Ascension

Scott Jenquin <scott.jenquin@ascension.org>

Ascension Technologies Security Training & Awareness Content - March 2020: Conducting work remotely and securely during the COVID-19 pandemic

1 message

Ascension Technologies Security <noreply@communications.ascension.org> Fri, Mar 20, 2020 at 9:09 AM
Reply-To: asecurit@ascension.org
To: scott.jenquin@ascension.org


You play a vital role in Ascension's information security
Read below to learn how you can help

Conducting work remotely - and securely - during the COVID-19 pandemic

Concerns about COVID-19 have changed the way many Ascension associates do their work. Unfortunately, along with that comes a treasure-trove of lures that cybercriminals have begun to use to perpetrate scams. Please review the tips below about the acceptable use of Ascension internet resources and safe ways to work remotely.

Watch for COVID-19 scam emails and sites: Scammers are taking advantage of the fear and confusion surrounding COVID-19 with new twists on phishing emails and fake websites. Beware of external emails containing links, attachments or urgent calls to action. If you are not sure an email is legitimate, delete it or use the *PhishAlarm* (*Report Phish*) button for your Ascension account. Don't click on links in pop-up ads or text messages. To find reliable information, visit familiar sites such as the one for the Centers for Disease Control and Prevention.

Share securely: For most associates, Google Drive is the only authorized cloud storage solution. Your supervisor will let you know if your team can use others. When sending confidential information to non-Ascension addresses, use *-secure-* or *-PHI-* in the subject line to encrypt the message. Never send Ascension data to your personal email; log into your Ascension Gmail instead.

Downloads to non-Ascension devices are blocked: If you need to work remotely, you can access Ascension's Google Suite products. However, you will be unable to download Ascension files to personal devices, and you may not print hard copies of Ascension data on your home printer.

Connecting outside the home: Be sure you are connecting to a legitimate network wherever you log in. Hackers often set up fake Wi-Fi connections in order to steal information. Avoid transmitting sensitive information over public networks, but if you must do so, ensure you are using an encrypted connection to the site such as with Ascension's G Suite products.

Adjust your router settings: Use a strong, unique password to secure your home Wi-Fi network and don't share it with anyone who doesn't need to use it regularly. Consider creating a separate guest network for visitors to use if your router supports it. Change your home internet router's administrator password to something known only to you and those who need to manage its settings. Use WPA2-AES encryption -- a security protocol that all modern routers offer as an option -- to protect your connections. Enable your router's built-in firewall functionality. Also, use a firewall on connected personal devices, such as personal computers. These settings already are configured on Ascension devices.

Ongoing router security tips: Rename your network's default name, its SSID, to prevent hackers from easily learning the brand and type of your Wi-Fi router. Disable universal plug 'n play (UPnP) unless you are actively using it to pair new devices to your home network. Finally, position your router to minimize signal leakage outside of your home. Don't place routers near windows, for instance, where the signal can be easily intercepted. There is no reason for you to manage your router from outside your home, so disable remote management to protect you from external attackers. And finally, when not using your router for long periods of time, turn it off.

Limit or secure connected devices: Don't needlessly connect devices to your home network. Many Wi-Fi-connected gadgets, such as refrigerators or other appliances, gain little additional functionality when connected while adding risk to your network. If you must add such devices, follow the same tips you used when securing your router: set passwords, update the firmware and shut these devices down when not in use.

VPN use: Some associates, including people managers, may require access to specific Ascension systems such as PeopleSoft and ServiceNow, as well as applications, network drives or devices through a secure network connection called a virtual private network (VPN). If you do not already have VPN access enabled, your manager can submit a request here: https://provisioning. ascensionhealth.org, but will need to log onto the VPN to access the site if outside an Ascension facility. Only request access if absolutely needed.

Tech support: Contact the Ascension Service Desk for assistance with Ascension-provided devices. The Service Desk cannot provide support or troubleshooting for personal devices such as home Wi-Fi routers. Consult your service provider, router manufacturer's website or YouTube for further tips on configuring personal devices.

For more guidance from Ascension on what you need to know about technology and working from home in response to the COVID-19 pandemic, review this document.

To learn more about information security at Ascension at any time, email your questions to the Ascension Technologies Security Training and Awareness team by choosing the *AscTech-MB-SecurityQuestion* mailbox from the email directory. Report questionable emails using the *PhishAlarm* button (formerly *Report Phish*).

Ascension Technologies

Email Security Resources | View online

Powered by Audience Engagement