FTI JOURNAL

ARTICLE

If You're Connected, Get Protected

October 2020

In the first of four articles for Cybersecurity Awareness Month (October), FTI Cybersecurity presents essential best practices for protecting your connected devices.

Internet-connected devices, programs, and apps are ubiquitous in today's world. Mobile phones, voice-activated speakers, and even smart thermostats all provide conveniences to our daily lives. But all that convenience comes with a price: It creates opportunities for hackers and malicious actors — whether experienced or not — to break into your devices without your even knowing it. Once inside, they can feast on data and information that puts your security, and by extension, your company's security, at risk.

In 2020, we are facing an unprecedented level of cyber vulnerabilities as our lives are powered by the Internet more than ever. We're on our desktop computers and laptops to engage in video teleconferencing. We're responding to email on our mobile phones late into the evening. By extension, our home Wi-Fi systems are getting a workout. To better protect yourself, here are steps to take to secure your devices.

Video Teleconferencing

Working from home and remote schooling has put video teleconferencing (VTC) front and center in our households. However, the software we download to our computers, tablets, or mobile phones to run VTCs creates endless entry points that malicious actors can exploit.

Protect It:

— **Ensure meetings are private.** It's best practice to protect your online meetings with a password for entry or by controlling guest access from a virtual "waiting room." This ensures there are no uninvited guests attending your meeting.

— **Keep meeting links confidential.** Do not publish your meeting link; send it only to the participants you expect to attend the meeting.

— **Use a virtual private network (VPN)**. A VPN is an encrypted connection from your device to a Wi-Fi network. There are several free or low-cost VPNs that are easy to install. They provide an additional layer of security by rendering your device's internet protocol (IP) address — the number sequence that identifies a device —anonymous from online snoopers.

— **Use two-factor authentication**. VPNs simply require a username and password for access; upgrading to two-factor or multifactor authentication adds greater protection.

— **Ensure VTC software is up-to-date**. VTC companies are continuously updating their software to maximize the latest features. But just like the operating system on your mobile phones, updates also add the newest security measures to ensure video calls are safe and secure.

— **Avoid "oversharing" your screen**. Be cautious during video teleconference meetings: If possible, close all active desktop windows to prevent accidentally sharing content not meant to be viewed by others.

Home Wi-Fi

Our Wi-Fi routers are pulling double duty in the work-from-home and remote school era. It goes without saying that you should be aware of the sites your children are connecting to as a basic step toward protecting your devices.

* Consult your device's operating manual for guidance.

Protect It:

— **Create a guest network**. "Network segmentation" is a great way to further protect your wireless network from trusted versus untrusted devices, such as school laptops and company devices. A guest network can also improve security when friends or family access your network.

— **Only visit secure websites.** You can recognize these by the designation "https" at the start of a site's URL address. (The "s" in "https" stands for "secure" and indicates that the page's owner has obtained an "SSL Certificate," which ensures a secure session with a web browser.) If you're not sure if a page or site is secure, navigate to your device's account settings and look for a section on security. Find the setting labeled "always use https" or "always use secure connection" and check that box.

— **Use antivirus software**. It's inevitable that some threats will get through. Antivirus software can act as the next line of defense by detecting, blocking, and even removing known malware in some cases.

— **Create a strong password**. This may be the oldest security recommendation in the book, but it remains the most essential and most easily overlooked. For guidance on best selections, see our article "Secure Your Data By Tightening Your Weakest Links.")

— **Enable WPA2.*** This refers to the encryption standard of your Wi-Fi system. The latest version, WPA2, or "Wi-Fi Protected Access 2," updates the version some Wi-Fi routers were shipped with (WEP or WPA). You don't need to know the technical details; you just need to visit your router's page on your computer and make sure your system is running WPA2.

— **Update firmware.*** Just like you update the OS on your phone to add new features and improve security, the same applies to your router. Visit your router's page to update.

AUTHORS

RON YEARWOOD
Senior Managing Director
+1 415 283 4267
ron.yearwood@fticonsulting.com

DAVE L. BEST
Senior Director, Cybersecurity
+215 605 4355
dave.best@fticonsulting.com