Internet Society

Keeping Your Workplace Safe Online

Don’t put yourself or your coworkers at risk!

Next Century Cities

For many of us the Internet is a staple in our day-to-day lives – especially at our jobs. But did you know that by simply connecting your device to WiFi or delaying computer and software updates can put you and your workplace at risk of a cyberattack?

Any time you go online you're using a gateway to the Internet. At work, this is usually either a WiFi or ethernet connection. When you connect a device to that gateway, it has a path to all other devices using that same gateway. That's why your mobile phone can sync with your smart watch. However, if gateways and devices are not secure, bad actors could also get access to your laptop and other devices using the same connection.

Don't put yourself or your coworkers at risk!

If you work for a company or agency that has sensitive or private information stored on its devices (especially in government or related services), it is critical to make sure that only secure, trusted devices have access to that network.

Here are 8 easy ways to help keep you, your colleagues, and your workplace network safe online.

1 Don't connect your Internet-connected smart devices to your work WiFi network.

If you connect an insecure or vulnerable device (like an knock-off watch or smart assistant) to your work WiFi network, it can be used to infiltrate the network as a whole.

Example: A fish tank thermometer was used by hackers[1] to steal a casino's database!

Fix: Leave your smart devices at home. If you need them for work, either connect them to a guest network or one that doesn't have access to the same devices where sensitive information is stored.

2 Don't use smart assistants in the same room where sensitive or private meetings take place.

Smart assistants are inherently insecure because their job is to constantly listen for a "wake" word that gives a command. They can also record what they hear – without your knowledge– and store it in company databases to help improve the service. If you're having sensitive conversations, they may be picked up, saved, and heard by employees of the smart assistant's parent company.

Example: Amazon Alexa employees may be listening to your conversations.[2]

Fix: Leave personal assistant devices at home. If you need to bring a smart assistant to work, disable the listening mode or make sure your colleagues are aware and place it in a place where conversations are public like a lobby.

3 Do your homework before buying a new smart device.

With the ever-growing number of connected devices hitting store shelves each year, it can be hard to tell which products were designed to keep you and your data safe online. Here are two tip sheets to help you keep security and privacy in mind when buying and setting up new devices.

Smart Device Purchase and Setup Checklist[3]
Enhancing the Security, Privacy, and Safety of Connected Devices[4]

4 Use unique passwords.

Using the same password for everything may be easy to remember, but it puts you at huge risk of a data breach and account hijack. If even one of your services is hacked and your password is discovered, it can also expose bad actors to your social media accounts, online banking, email, work systems, and more.

Example: Millions of passwords and corresponding usernames (email addresses) have already been hacked[5] and can be used to unlock the owners' accounts.

Fix: Use a password manager to create strong and unique passwords for your accounts. The system will save them for you and can auto input them when you log in to your accounts. To access the database of passwords, you only need to remember one master password that you create yourself. This way, you stay safe without having to keep a rolodex of passwords in your brain! Where possible, you should also use two-factor authentication[6] (e.g. password plus a code from an app like Google Authenticator).

5 Don't click on links in emails or messages unless you're 100% sure they're safe.

Phishing scams are some of the most common ways online criminals can get access to your network and contacts. Hackers will spoof or mimic an email address or messaging account you trust (usually family, friend, or a coworker) with an attachment or a link to something for you to click on. When you do, the hacker can use it to download malicious software to your computer, steal your information, and get your passwords and other sensitive information.

Example: Check out this guide[7] on how to avoid phishing schemes from the Federal Communications Commission.

Fix: Turn off automatically loaded remote content. Only click on links (in messages, emails, or even social media) if you're absolutely confident that the person that sent it actually sent it. If the URL looks suspicious, that's a red flag. When in doubt, don't click on the link. Use bookmarked URLs to log on to your bank, medical practices and other sensitive sites instead of links within an email.

6 Promote the use of strong, encrypted devices and resources at work.

Unencrypted or weakly-encrypted devices and services can put your personal and work data and systems at risk. Encryption is one of the strongest tools to protect our data, privacy and critical systems online. Encrypted devices and systems are much harder for malicious actors to access, and even if they did, it makes the information unreadable without your personal "key" to unlock its contents.

Example: In 2014 Sony was hacked[8] and all of its employees unencrypted private emails, passwords, and in some cases Social Security Numbers were publicly released.

Fix: Use services that promote their use of strong encryption, especially end-to-end encryption. When transferring or beginning your use of a new service or software, be sure to check if they automatically encrypt your data and messages, or if you can turn on that feature. If not, consider using another service.

7 Keep your software up to date.

Updates don't just come with new features. They are a developer's way of fixing any known bugs or security vulnerabilities in their software. Companies are constantly working to keep their software stronger than the best hackers out there. Waiting for your computer and devices to download, install, and reboot after an update may be annoying, but it is a critical way to protect yourself from the most current security threats. Delaying software updates can unnecessarily put you, your devices, and your entire network at risk of a cyberattack.

Example: Every day there are reports of security vulnerabilities that need to be patched. Take Microsoft for example.[9]

Fix: Set aside time for updates – they are important. Use the time to organize your desk or get some face time with colleagues.

8 Back up your files.

We're increasingly hearing stories of government departments, municipalities, hospitals and other critical institutions falling victim to ransomware attacks. This is when a hacker blocks access to your files, systems, and saved information until a ransom is paid.

Example: A 2018 ransomware attack[10] in Atlanta, Georgia impacted City Hall and law enforcement departments for nearly five days. In 2019, three hospitals[11] in Alabama had to turn away patients.

Fix: Regularly back up your files, preferably with both a cloud provider and an external physical storage device. Disconnect the backups from the computer and the network, and remember to check that your systems can recover from those backups. This is especially important for those working with irreplaceable, private, or time-sensitive information in places like government offices, medical professions, and critical infrastructure.

Endnotes

1 https://www.businessinsider.com/hackers-stole-a-casinos-database-through-a-thermometer-in-the-lobby-fish-tank-2018-4
2 https://www.bloomberg.com/news/articles/2019-04-10/is-anyone-listening-to-you-on-alexa-a-global-team-reviews-audio
3 https://www.internetsociety.org/wp-content/uploads/2019/04/smart-device-checklist.pdf
4 https://www.internetsociety.org/wp-content/uploads/2019/04/iotchecklist.pdf
5 https://www.forbes.com/sites/kateoflahertyuk/2019/04/21/these-are-the-worlds-most-hacked-passwords-is-yours-on-the-list/#71cc35d289cc
6 https://twofactorauth.org/
7 https://www.consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams
8 https://time.com/3639907/sony-hack-data-security/
9 https://thenextweb.com/security/2019/09/24/microsoft-issues-emergency-windows-patch-to-address-internet-explorer-zero-day-flaw/
10 https://www.govtech.com/security/What-Can-We-Learn-from-Atlanta.html
11) https://www.bbc.com/news/technology-49905226