4.8. Security Toolkit: Other Tips on Technology Setup

Updates and Patching

IT staff should ensure that all software is up to date and properly patched. This can include device policies that push updates to all computers, but it should also include updates to core applications (e.g. case management systems). This might also require upgrading hardware as well, since older computers might not be able to support new software.

User Accounts

Whenever creating user accounts on computers or in technology systems, IT staff should create standard accounts, not admin accounts. Every user should have a standard account. When a user needs admin level access, IT staff should create a separate account. IT should also have policies for onboarding and offboarding staff to ensure that former staff do not retain access to accounts after they depart.

Wi-Fi

Staff should be trained not to use key applications over public Wi-Fi while outside of the office. Public Wi-Fi can be unencrypted and might reveal private data and information to others sharing that network.

Inside the office, you should separate your private staff network from your guest network. This way, outside users do not use the same Wi-Fi network that is handling your sensitive data and applications. You can also configure your Wi-Fi network with more security features, such as connecting users to your wireless network with unique logins or segmenting your network depending on the user or group permissions by using VLANs.

Remote Work

When building remote work technical capacity for staff and volunteers, it is helpful to start with the development of policies or protocols for remote work so that the organization build the right capacity, functionality, and security into the environment. If the organization already has remote work technology in place, it is still worth developing the policy and then work to comform the technology to support the policy. Have a telecommuting policy and have policies that explain how to use personal devices. This should include policies on which applications your staff are allowed to use and how to use them. You should also establish a communication plan for how to share information with your staff. Invest in the right technology tools to make remote work as secure and successful as possible.

You should also have a security plan for any remote work. In general, users should only be using the equipment provided by your organization to secure your data. Consider the other topics in this toolkit, as they can be even more important in remote settings (e.g., MFA and password policies). You can also use virtual private networks (VPNs) for remote access, which can provide direct secure access to your on-site technology even while off-site.

Securing Home Technology

Legal aid staff members and volunteers, working from home are typically working in an environment with other users (e.g., family members, roommates, partners) and many different Internet-enabled technologies (e.g., desktops, laptops, tablets, smartphones, printers, Wi-Fi access points, routers, cable modems, game consoles, smart TVs, smart speakers, smart thermostats, home NAS/server, connected appliances, and IP cameras). It is important generally advisable that all equipment in the home be kept up-to-date with current software and firmware (a type of software that get more directly controls and manages specific hardware such as a router or a printer). Keeping equipment up to date helps protect legal aid and personal user data and systems as the updates frequently fix security bugs in the software or firmware. Typically, every equipment manufacturer has a website with current software and firmware to download. As needed, users should work with the equipment manufacturer's tech support to make sure they successfully are successfully updating their equipment. Users may also have equipment that is no

longer supported (updated) by the manufacturer. Manufacturers may refer to such equipment as end-of-life hardware or equipment. When equipment is no longer support, newly discovered security risks for that equipment will not be fixed by the manufacturer which in turn makes the equipment more vulnerable. That equipment should ideally be replaced as soon as budget and time allow.

In addition to keeping equipment up-to-date, it is important that the equipment be configured securely. At a minimum, this would mean changing all default passwords to a new, more complex, longer password. It would also mean turning off any functionality that isn't needed (if a user has a home network attached storage (NAS) server for photos, videos, files, and backup that server might also have a built-in web server that is not being used and should be turned off) or leaving devices disconnected if not needed (e.g., if a user prints via a USB cable to their printer, they could turn off the printer's built in Wi-Fi connection). For network access devices such as cable modems, firewall, routers, and wireless access points, it is particularly important that users read all the documentation and communicate with the manufacturer or Internet provider's tech support to ensure that their configuration is as locked down as possible while allowing needed access for equipment inside the household.

While all equipment in a household may pose security threats to the user's work machine, users should pay particular attention to updating and securely configuring their cable modems, firewalls, routers, wireless access points, and other computers, tablets, and smartphones. For laptops and desktops, users should be running current anti-virus, anti-malware software from a trusted vendor and use built-in security configuration checks. Microsoft includes such tools in Windows 10 and 11 (Windows Security). Users might also consider security software for the tablets and smartphones.

Last updated on December 15, 2023.

Print

Table of Contents

NEWS

News & publications

The news about recent activities for needed peoples.

More News

24 Mar 2023

Project Spotlight: UpToCode

Because everyone has a right to a safe home, Northeast Legal Aid (NLA) is...

Continue Reading

28 Feb 2023

Member Spotlight: Josh Lazar

We are heading south to Florida today to meet community member Josh Lazar, the...

Continue Reading

Our Partners


MAP
MICHIGAN
ADVOCACY
PROGRAM
LSC
America's Partner
for Equal Justice
LEGAL SERVICES CORPORATION