LOVE LAW
FIRM PLLC

PROTECTION ON THE GO
3 Threats & Responses

Three of the greatest threats facing businesses with mobile workforces, especially when the employees use their personal smartphones, tablets and laptops, are the use of open access Wi-Fi, the lack of proper password protection on those devices, and the failure to keep devices updated with the latest software and security patches.

Open Access Wi-Fi

Surprisingly, despite repeated warnings, most people remain ignorant of the dangers posed by public Wi-Fi service found in cafes, libraries, airports, hotels and the like. When people log onto the internet, surveys indicate that they immediately begin checking email, posting on social media and logging into their bank accounts. These activities include the transmission of passwords and other sensitive personal information.

To protect against open access Wi-Fi, there are several things employees can do. They can create a virtual private network (VPN) which encrypts data transmitted over the network. To set up a VPN on a smartphone or tablet, there are apps that can use to do so easily and securely. Employees can make use of SSL connections by enabling the “Always use HTTPS” option on websites visited. This option can be found in the settings area of the device. When in public, employees should turn off Wi-Fi automatically to avoid any open backdoors, even if they are not using the Wi-Fi.

Improper Password Protection

People are inundated with devices, sites and applications that require passwords. Unfortunately, it is well known that *even among those educated about the risks*, people routinely use the same password for the vast majority of their accounts. This means that if a malicious entity acquires one password, nearly all are comprised. The impact of such a breach can take months or even years to fully play out.

Employees need to be required to have strong, unique passwords on and for their devices, sites and applications. Strong passwords are longer (at least 8 characters), use combinations of upper and lower case letters, numbers and special characters. Companies need to create policies requiring such usage and actively coach employees how to achieve compliance. There are numerous good applications now that help track and store passwords so that personnel can use unique ones in all instances.

Failure to Update Devices

No piece of software is perfect. Computer programmers have long realized that continual improvement is required as hackers and other malicious actors look to exploit weaknesses in products. This is why devices routinely show that updates are available for the operating systems, applications and programs being used. Unfortunately, many people ignore these updates or delay implementing them because they require the device to be offline for some period of time, to be connected to power, or some other inconvenience to the user.

Without proper updates and patches, smartphones, tablets and laptops are vulnerable. While traditionally Apple products have been less impacted by such problems, several recent incidents have shown that its immunity is not fail-safe. Companies need to require that personnel implement all updates as they become available in order to maintain network security.

—By Francine E. Love, LOVE LAW FIRM, PLLC

Francine E. Love is the Founder & Principal Attorney at LOVE LAW FIRM, PLLC which is dedicates to serving the entrepreneur and small business owner. The opinions expressed are those of the author. This article is for general information purposes and is not intended to be and should not be taken as legal advice. To learn more about Love Law Firm please see our website, www.lovelawfirmpllc.com, or call us at 516-697-4828.