



US-CERT

UNITED STATES COMPUTER EMERGENCY READINESS TEAM

The Risks of Using Portable Devices

Pennie Walters

Portable devices like jump drives, personal audio players, and tablets give users convenient access to business and personal data on the go. As their use increases, however, so do the associated risks. The properties that make these devices portable and enable them to have on-the-fly connection to various networks and hosts also make them vulnerable to losses of physical control and network security breaches. Using portable devices can increase the risk of data loss (when a physical device is lost), data exposure (when sensitive data is exposed to the public or a third party without consent), and increased exposure to network-based attacks to and from any system the device is connected to (both directly and via networks over the internet).

About Portable Devices

Business and home users can choose from many types of portable devices, and new products are always arriving on the market. This paper focuses on two subsets of portable devices:

- simple media devices that require a wired connection to a host in order to transfer data. (for example, jump drives, media cards, CDs, DVDs, and music players without Wi-Fi capability)
- smart media devices that can transfer data with a wired or non-cellular wireless connection (for example, tablets, gaming devices, music players with Wi-Fi capabilities, and ereaders). These devices are generally used to access email, surf the web, and download applications, music, and books.

Smart phones and laptops are also portable devices, but we don't discuss them in detail here. You can learn more about the threats to smart phones at http://www.us-cert.gov/reading_room/cyber_threats_to_mobile_phones.pdf and about protecting laptops at <http://www.us-cert.gov/cas/tips/ST04-017.html>.

What Are the Risks?

Using simple storage media may seem innocuous, but it has the potential to cause many problems for a user or an organization. TechAdvisory.org reports that 25 percent of malware (malicious programs) is spread today through USB devices. These devices (such as a jump drive or music player) plug into the USB port of your PC and may contain malware that you copy

unknowingly or that gets launched automatically by the Autorun or Autoplay feature of your PC. And attacks are growing even more sophisticated and hard to detect as attackers use small circuit boards inserted in keyboards and mouse devices to launch malicious code when a certain key is pressed or condition is met. Once malware infects your PC to steal or corrupt your data, it might spread to other PCs on your home or organizational network. And these devices are an easy way for attackers to quickly propagate malware by passing it across all PCs that the device connects to. Because these storage devices can install malware inside of any firewalls set up on your PC or network, you might not detect the malware until major damage has been done. Storage devices can also give malicious insiders the opportunity to steal data easily and inconspicuously because the devices are easy to hide and their use is hard to track.

Smart devices also have the potential to surreptitiously infect your PC or network when you download applications or games containing malware or viruses. Their use by a large population, emphasis on usability, and immature security tools make them ripe for malware attacks. Also, the potential for irreparable data exposure or loss arises from practices commonly used for storing sensitive data on smart devices. For example, users frequently keep personal bank account numbers or proprietary client information on their smart device that may be running untrusted applications or be connected to untrusted and vulnerable networks.

In addition, the features that make smart devices so attractive—such as Bluetooth and Wi-Fi—can also pose the most risk. When Bluetooth is on, the device becomes “discoverable” to both your headset *and* malicious attackers seeking to exploit the connection. They also target home and public Wi-Fi networks; public Wi-Fi hotspots are especially risky and a frequent target of attackers looking for data to pilfer. Attackers often linger nearby and use tools such as Kismet and Wireshark to intercept unencrypted data.

Another potential risk with both storage devices and smart devices comes from their small size and portability. You can easily leave them at a café or in a cab, and never see them or the data stored on them again. And if they contain sensitive or proprietary organizational data, your company’s reputation and well-being—and yours—could be in serious jeopardy.

What You Can Do to Minimize These Risks

Whether you are a home user or work in an organization, there are things you can do to reduce the risks associated with using portable devices. Recommended best practices for individuals and organizations are listed below.

Recommended Practices for Portable Storage Media

Follow these best practices when using storage media such as jump drives, CDs, and music players without Wi-Fi capability:

- Install anti-virus software that will scan any device that connects to your PC via a peripheral port (such as USB).
- Never connect a found jump drive or media device to a PC. Give any unknown storage device to security or IT personnel near where you found it.

- Disable the Autorun and Autoplay features for all removable media devices. These features automatically open removable media when it's plugged into your USB port or inserted into a drive.
- Keep your personal and business data separate. Don't plug your personal audio player into your work PC or your work jump drive into your home PC.
- Secure all sensitive data stored on jump drives, CDs, and DVDs using strong encryption, such as AES 128/256 bit.¹ Also be sure to have a backup copy located in a secure location.
- On your PC (and all PCs on a network), set up a firewall and install anti-virus and anti-spyware software. Enable automatic updates or otherwise ensure all software on your PC stays up to date with current patches.
- When you have finished transferring sensitive data from a USB drive, be sure to delete it using a secure delete utility.
- Consider using jump drives that have an onboard anti-virus capability, which automatically scans both the drive and any computer you plug it into. Although such a capability can take substantial disk space and time to run, it may be worth using, depending on your situation.

Recommended Practices for Portable Smart Devices

Follow these best practices when using smart devices such as tablets, music players with Wi-Fi capability, and ereaders:

- Password protect the device using a strong password or PIN, and change it periodically. (To learn more about passwords, go to http://www.us-cert.gov/reading_room/PasswordMgmt2012.pdf.)
- Before downloading applications and games, find out what they will have access to on your device. Most applications provide that information; avoid downloading any that don't.
- Download applications, games, and music only from trusted sources. For example, only download well-known games from reputable and verified vendors or from the commercial store backed by your device manufacturer or provider.
- Run anti-malware software on the device and take the appropriate action when it identifies suspicious applications. Also, scan the entire device periodically for malware.

¹ You can learn more about AES encryption by watching the video at <http://technet.microsoft.com/en-us/windows/dd408739>, going through the tutorial at <http://www.truecrypt.org/docs/?s=tutorial>, or reading the AES guide at <http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf>.

- When possible, set up a local firewall on the device to filter inbound and outbound traffic and block malicious software.
- Set an idle timeout that will automatically lock the device when you're not using it.
- Do not "jailbreak" the device. Jailbreaking is removing the limitations imposed on a device by the manufacturer, often through the installation of custom operating-system components or other third-party software. Jailbreaking makes a device more vulnerable because it removes important safeguards against malware.
- If your device supports location tracking, activate global positioning system (GPS) functionality so you can track the location of your device if you misplace it.
- Disable Bluetooth, Wi-Fi, and other services when you're not using them.
- When using Wi-Fi, be sure to encrypt your home network, use a VPN connection, or otherwise ensure that traffic is encrypted when you're in a semi-trusted environment (for example, when you may trust the wireless access point but not necessarily the other users on the network).
- When using Bluetooth, set it to "non-discoverable" mode to make the device invisible to unauthenticated devices.
- Secure all the data stored on tablets using AES 128/256-bit encryption. Also be sure to have a backup copy of the data stored in a secure location.
- If available, enable a remote-wiping feature to erase all data on the device if you misplace it.

Recommended Organizational Practices for All Portable Devices

Organizations should follow these best practices for managing all types of portable devices:

- Limit the use of all removable media devices except where there is a valid business case that has been approved by the organization's chief IT security officer.
- Create security and acceptable-use policies for all portable media devices, and educate your employees about those policies.
- Teach your employees to report missing devices immediately so they can be wiped of all data.
- Choose only a few devices to support, and consider their security features and vulnerabilities.
- Educate employees about the value of using strong passwords and PINs, and require their use.
- Only allow access to the organizational network through a secure VPN connection.

- Consider banning personal, portable media devices (that is, those that can't be controlled and monitored by the organization) from the workplace.
- Configure secure sockets layer (SSL) security features on organizational web servers to encrypt data being transmitted.
- Consider the costs and benefits of distributing locked-down, corporate-controlled devices over implementing a "bring your own device" policy.
- Consider implementing an inventory of mobile devices that may carry sensitive company information, and auditing it on a regular basis.

Conclusion

Using portable devices comes with both value and risks, but those risks can be mitigated or at least reduced if you follow the best practices outlined in this paper. As existing products evolve and new ones enter the market, you must use them with caution, always considering their security features, possible vulnerabilities, and ways they could be targeted by malicious attackers.

Further Reading

"Protecting Portable Devices: Data Security," Security Tip ST04-020

<http://www.us-cert.gov/cas/tips/ST04-020.html>

"Protecting Portable Devices: Physical Security," Security Tip ST04-020

<http://www.us-cert.gov/cas/tips/ST04-017.html>

"Cyber Threats for Mobile Phones"

http://www.us-cert.gov/reading_room/cyber_threats_to_mobile_phones.pdf

"Password Security, Protection, and Management"

http://www.us-cert.gov/reading_room/PasswordMgmt2012.pdf

"Federal Information Processing Standards Publications 197: Advanced Encryption Standard"

(AES) <http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf>