

Simple Steps to Safer Devices

By following some simple steps, consumers can protect their data privacy when using electronic devices.

Consumers of all ages are using more and more digital devices to do more than just check their email. Today, devices are used to do things such as: access the internet, carry out banking transactions, social networking, and shopping. For children and adults alike, using these wonderful devices brings some unwanted risks.

Here is what consumers need to do to keep information secure on those devices:

Protecting a computer or laptop

Every computer and laptop needs:

- **Strong security software.** Any computer that is linked to the internet will be infected if it isn't protected. Whether you use a Windows PC, or a Mac, *all* computers and laptops need security software. When Apple devices were a tiny minority of the total market, designing malware to attack them wasn't very lucrative, but those days are long gone; iUsers are now profitable targets.
- **An active firewall.** Computers come with firewalls (a set of programs located on your computer that protect it from being accessed by other computers). These firewalls are turned on by default, **don't turn the firewall off!**

Additional considerations if the computer/laptop is used by a minor:

- Consider the full range of functionality the computer or laptop offers. Are there features that should be turned off—like location tracking? Webcam chats? iKeepSafe recommends that computers used by minors should be secured with filters and parental controls such as [K9 Web Protection](#) or [Norton Online Family](#). These provide a safer experience for youth and protect your machine from unwanted malware.
- iKeepSafe also recommends that parents maintain administrator control of computers, giving children a “limited access” account. This will prevent children and friends from inadvertently downloading malware and illegal content.
- Talk with your child. Make it clear what is and is not acceptable use of the device, including times of day the device is used, the ethical treatment of others, the types of downloads permitted, and so on.

Replacing or donating a computer or laptop

Remember to remove all your information from your hard drive. An old computer is likely to have stored a great deal of sensitive information including financial data, personal information, passwords, addresses and phone numbers, photos, medical information, and so on.

- Start by backing up any information you want to keep like files, music, photos, calendars, contacts, website locations, applications, account information, passwords, etc., to a form of storage like an external hard drive, a CD-ROM, a USB (flash) drive, or your new computer.
- Then, use a utility program that wipes all the information off a hard drive – there are several of these programs to choose from and they can be purchased in computer stores or online. You may want to run the utility several times in order to be sure that the information cannot be retrieved.
- When cleaned of your information, look for organizations or charities in your area that collect old computers, resell it online, or take it to a recycling center that knows how to separate the hazardous materials from the rest of the parts.

Protecting a wireless network

Don't forget to set it up according to the user manual; be sure to create a new username and a strong, unique password.

- It is also important to help consumers understand they need to be cautious when using public WiFi services as these may or may not be safe.

Protecting a smartphone

Cell phones were the number one item on tech wish-lists this holiday season.

Unfortunately, the majority of smartphone users don't understand that these internet-enabled devices are prime targets for cybercriminals—in part because users remain so unprotected. Research shows 72 percent of smartphone users have no protection against malware on their devices, leaving data stored on these devices vulnerable.

It is estimated that 24 percent of users have passwords stored on their mobile devices. This is particularly concerning when nearly 32.5 million Americans now access their banking information through their smartphones. In addition to these risks, 113 mobile phones are lost every minute in the U.S. leaving personal information in the hands of whoever picks up the phone.ⁱ

- Create a unique password to prevent unauthorized access to devices.
- Install quality mobile security software. Sadly, some free security tools fail to protect users at all). To find the right product, look online for reviews and comparisons of security software for the type of device you're using. Set the software to automatically update.

Additional considerations if the smartphone is used by a minor:

- Know the device's security features, and what additional security, safety, or privacy add-ons may be available.
- Consider the full range of functionality the phone offers. Are there features that should be turned off—like location tracking? All of the major cell phone providers offer no-cost filtering and more robust parental controls for a small fee. These will provide a safer and more monitored experience for youth.
- Request that the sales clerk help you set up the phone with the appropriate safety and security features.

- Talk to your child. Make clear what is and is not acceptable use of the device, including times of day the device is used, the ethical treatment of others, the types of downloads permitted, and so on.

Protecting a game console

There's plenty of entertainment to be had from a game console. Keep in mind that all game consoles have the functionality to access the internet and connect users with new people. So, if the console will be used by minors, consider what additional precautions—if any—your child needs.

Additional considerations if the game console is used by a minor:

- Look at the console's security and safety features, and determine what additional security, safety, or privacy add-ons may be available.
- Consider the full range of functionality the console offers. Are there features that should be turned off—like location tracking or Webcam chats? Or services that should be turned on like family safety (also called parental control) tools to provide a safer and more monitored experience for youth?
- Talk to your child. Make it clear what is and is not acceptable use of the device, including the types of games that will be appropriate, times of day the console may be used, what requirements you have regarding the ethical treatment of others, the types of filters in place for any web surfing, and so on.

Protecting a tablet

Tablets are in high demand and it's no wonder; tablets open the door to literally thousands of apps, games, and tools, as well as millions of websites.

- Tablets can be protected from malware and adult content with free apps, like [K9 Web Protection](#). Do your research to understand what security measures are in place. Tablets are often as capable as laptops and computers and face the same threats from malware.

Additional considerations if the tablet is for a minor:

- Many parents are caught off guard by the richness of tablet features like wireless internet connectivity, the ability to download thousands of applications which may—or may not—be suitable for your child, the 'always on' status of these devices, features like webcams that allow for video chats, and the ability to access any website—including any social networking site, and more.
- Consider the full range of functionality the tablet offers. Are there features that should be turned off—like location tracking and web chatting? Or are there services that should be added like family safety (also called parental control) tools to provide a safer and more monitored experience for youth?
- Talk to your child. Make it clear what is and is not acceptable use of the device, including times of day the device is used, the ethical treatment of others, the types of downloads permitted, and so on.
- It's worth noting that the iPad is the only tablet with built-in, easy-to-use safety settings, but all tablets can be enhanced with filtering and monitoring apps.

Protecting an e-reader

E-readers are fabulous items for bookworms (and future bookworms) of all ages. However, it is important to understand all of the device's features and determine whether the e-reader is appropriate for the user.

Additional considerations if the e-reader is for a minor:

- Know the device's security features, and determine what additional security, safety, or privacy add-ons may be available.
- Many parents are caught off guard by features like wireless internet connectivity, the ability to download more than just books—many e-readers can download games, apps, music, social networking sites and more. You may want to block or filter internet access for younger users. Parental control software such as K9 Web Protection or Norton Online Family will also help you manage times of day for access.
- Talk to your child. Make it clear what is and is not acceptable use of the device, including times of day the device is used, the ethical treatment of others, the types of downloads permitted, and so on.

Protecting a flash drive or other removable storage device

Everyone can use a little extra storage, especially when portability is crucial. To keep the gift recipient safer, you may want to select a flash drive that has pre-installed security software.

The proliferation of internet-enabled devices offers consumers convenient, quick ways to carry out daily activities. With a few steps, consumers can protect these devices and minimize the risk to their personal data stored and sent on these devices.

#

For additional information:

Jennifer Finlinson

iKeepSafe

Jennifer@iKeepSafe.org

(801) 623-3009

ⁱ A new study conducted by the National Cyber Security Alliance (NCSA) and McAfee