

# GOT A NEW PC, MAC OR MOBILE DEVICE?

Here's how to protect it and use it safely.



Introduction

02 >>

Six good habits to secure your devices

04 >>

Top online threats to avoid

06 >>

Smartphones need security, too

08 >>

12 >>

Protect your new devices with security by Norton

Stay in the know with Norton

13 >>

# You got a brand-new device. Congratulations!

We know how exciting it is ... slicing open the shrink-wrap, unboxing your shiny new tech from its sleek packaging. You can't wait to check out all its cool features and show it off to your friends. There's a certain joy that a new device brings. When you're so excited and happy to have a brand-spanking-new device that you don't even think about how to keep it that way—not just on the outside, but on the inside where the important stuff is stored.



## It's time to shake off that euphoria.

We know. It's hard to come down off that new hardware high, but let's get serious about device protection and make a promise to secure your new shiny tech and all those emails, photos, and accounts on them that *are* your digital life. Of course, cybercriminals would prefer that you don't, because they love easy access to information on unprotected PCs, Macs, smartphones, and tablets.

Ready? This eBook gives you simple tips on how to keep your new device protected and how to use it safely online. **Let's get started!**

# How to stand securely apart from the crowd

You're not alone if you haven't yet secured your device. Many people don't protect their devices simply because they don't think they need to.<sup>1</sup> However, that's far from the truth. In 2016, the Norton Cyber Security Insights Report revealed that 689 million people in 21 countries experienced cybercrime in a one-year period. In the U.S., alone, 106.6 million people were victims.<sup>1</sup>

Let's do the math. In the U.S., 35% of people have at least one unprotected device.<sup>1</sup> And in 2015, the average U.S. household owned 5.2 connected devices.<sup>2</sup> That means potentially 4 devices per household do not have any type of security on them. It's no wonder that cybercrime is on the rise.

Of those who do not protect their devices, 27% said they don't do anything "risky" online so they don't need protection.<sup>1</sup> When you consider how much we all do online that involves personal information—emailing, banking, shopping, setting up accounts—everything starts to look risky. But aside from not installing security software, some people aren't taking even basic steps to secure their devices and accounts, like using auto-lock settings and passwords.

Survey results published in the **2016 Norton Cyber Security Insights Report** show:



**Learn some good habits** to set yourself apart from those who are creating more risk to themselves by not protecting their devices.

# 6 good habits to secure your PCs, Macs, smartphones, and tablets

- 1 Install comprehensive security software.** Choose Internet security software that protects your PC or Mac against malware, ransomware, and zero-day viruses. The most complete security suites will back up and restore your files, and even protect mobile devices. For mobile devices, in particular, choose software that can remotely lock and wipe them if they are stolen or lost.
- 2 Back up your data.** Make it a habit to regularly back up your laptop, tablet, or smartphone to the cloud or a portable storage device. Otherwise, if your device is damaged, lost, or stolen, you might also lose your contact numbers, treasured photos and videos, and important financial and work documents.
- 3 Lock your device with a password/passcode.** At a bare minimum, you should always lock your device to prevent others from accessing your online accounts or other private information. Ensure your **password is strong** by using at least eight characters, including uppercase and lowercase letters, numbers, and symbols. For extra security, choose **two-factor authentication** for your online accounts whenever possible.
- 4 Guard your personal information.** Identity theft is a crime of opportunity that can be prevented by limiting exposure of your personal information. Only transact on secure websites. Make sure URLs begin with HTTPS, show a lock symbol, or display text in green—all indicate a secured site. Avoid phishing scams by being cautious about clicking links in emails, social media, or texts. **Be careful about what personal information you divulge on social media sites.** Never send personal information, such as credit card or Social Security numbers, via email, text, or instant message, or across social networks—especially on **unsecured public Wi-Fi**.
- 5 Download apps from trusted sources.** **Avoid apps from third-party sites.** The best-known app stores—such as Google Play and the Apple App Store—all have strict app submission and review policies to ensure apps are safe and not malware in disguise. App Advisor, a feature of Norton Mobile Security, lets you know if an app is safe or not before you download it.
- 6 Disable Wi-Fi, Bluetooth, and geo-tagging.** Prevent your mobile devices from connecting to unknown networks and devices by turning off Wi-Fi and Bluetooth when you aren't using them. Disable your device's geo-tagging feature, which identifies the location where photos are taken, allowing someone else to track your movements if the photos are published online.

## 3 easy ways to protect your new device



Set your device to  
**lock automatically**  
when idle.









Enable fingerprint recognition  
features, like **touch ID**.



Create a **strong**  
**passcode** or password  
for each device.

# Top online threats to avoid

Hacker Method	How It Works	Devices Impacted
<b>Malware</b>	Malware is software created to do harm. It includes computer viruses, worms, and Trojan horses. It also includes apps for mobile devices, such as those running Android and iOS operating systems.	 <b>Every device connected to the Internet</b>
<b>Phishing</b>	Phishing scams try to get you to divulge your personal information by posing as legitimate entities such as banks, online payment companies, or social media sites. Most people aren't truly sure how to tell a real email from a phishing email. Only 4 in 10 are doing it the right way by looking to see if the email is asking them to take a compromising action, like downloading attachments or entering login information. <sup>1</sup>	 <b>Every device connected to the Internet</b>
<b>Social media scams</b>	Hackers use fake offers—the most common form of social media-based attacks—to steal personal information or infect a device with malware. Social network users are invited to join a fake event, download an app or music, or enter a contest. Users are often asked to give their account login information or text a premium rate number.	 <b>Every device connected to the Internet</b>
<b>Identity theft</b>	Criminals use phishing scams to trick you into releasing personal information so they can steal your identity. Lost or stolen devices, or old devices that aren't wiped clean, can also provide thieves with what they need.	 <b>Every device connected to the Internet</b>
<b>Ransomware/ crypto-ransomware</b>	Ransomware is malware that renders your computer unusable, unless you pay the hacker to unlock it. Crypto-ransomware is even nastier because it encrypts your data.	 <b>Mostly PCs, laptops, notebooks, but also mobile devices</b>
<b>Public Wi-Fi</b>	Hackers exploit unsecured public Wi-Fi networks to intercept email messages, passwords, login credentials, or any other unencrypted information. Some hackers even create rogue hotspots that have seemingly legitimate names, such as "Official Airport Wi-Fi," so they can eavesdrop on all of your online activities and steal your personal information.	 <b>Mobile devices you use outside of your home, such as laptops, notebooks, tablets, and smartphones</b>



## How to gift—and wipe—your old device

Since you've been lucky enough to buy or receive a brand-new device, you might consider giving away your old one. Before you do, make sure you aren't passing along your private information along with your hand-me-down. You'll want to clean the device of any content, including personal files, saved passwords, or stored credit card information.

**Mobile phones or tablets.** Clean your device by resetting it or restoring it to factory settings.

**PCs, Macs, or laptops.** Wipe any content by reinstalling the operating system.

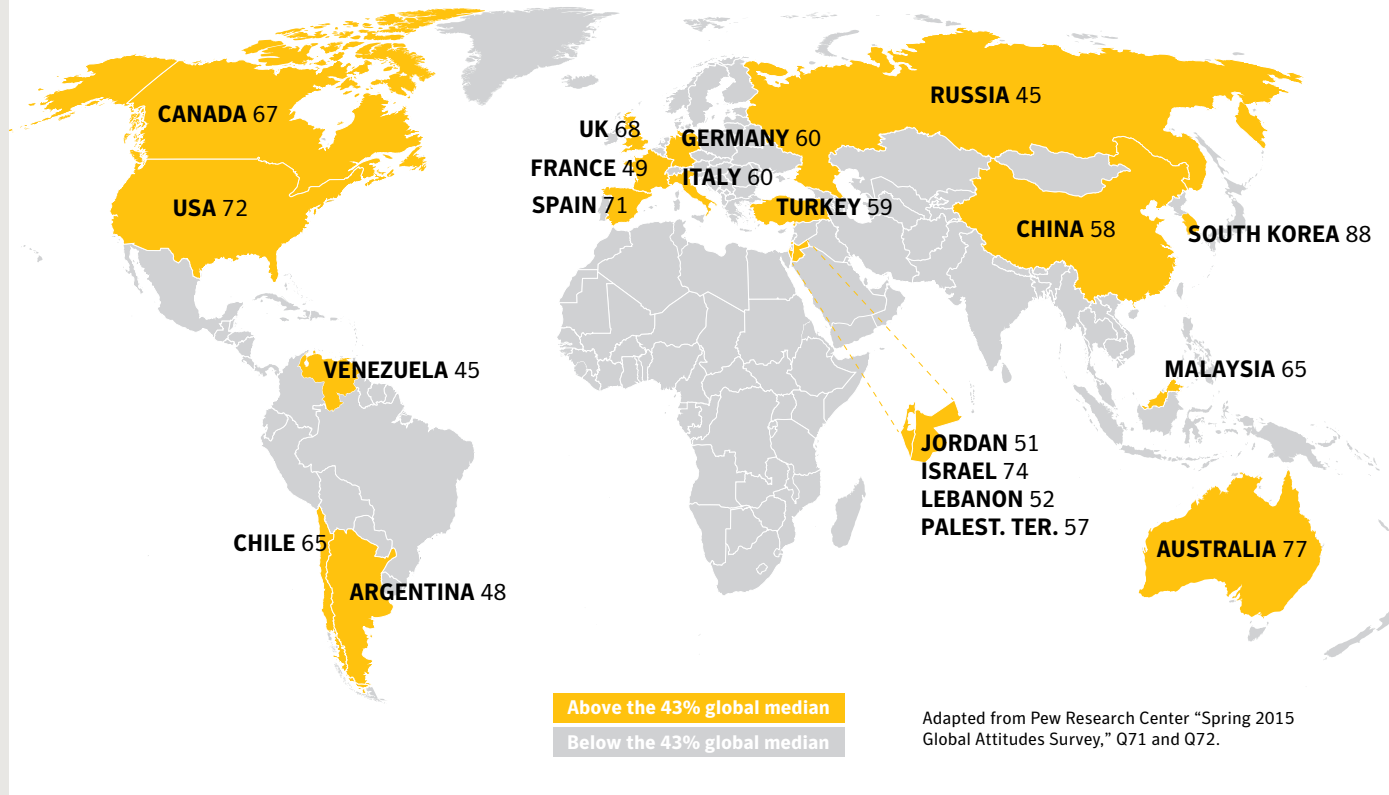
**For more information:**

[Let Go of Old Tech Securely and Responsibly](#)

[Keep Everyone Protected When Handing Down Mobile Devices](#)

## Smartphones are common in the United States and Europe

(Percentage of adults who report owning a smartphone)



## Smartphones need security, too

The number of mobile devices is growing globally. Smartphones, in particular, are becoming ubiquitous in many parts of the world, including the U.S.<sup>3</sup>

Smartphones are increasingly attractive targets for criminals because of the information they hold and their vulnerabilities. Cybercriminals are devising more sophisticated attacks to steal valuable personal data or extort money from victims.<sup>4</sup> No operating system is truly safe; both Android and iOS platforms have seen growing numbers of attacks.



# The dangers of malware apps

## Malware apps can:



Track your device's location



Divert texts from your bank



Collect device information



Use your device's microphone and camera to monitor your activities



Make charges to your phone



Download and install apps and files



Steal your personal information



Message your contacts



Hand over control of your device to a cyber attacker

# Top 5 tips for safer sharing on #social

Globally, Internet users spend almost two hours a day on social media.<sup>5</sup> If you're a frequent social networker, you may not realize that over-sharing by posting too much information can compromise your safety—or your family's and friends'.

**Follow these tips for safer online sharing.**



## **Check your privacy settings on your social networking sites.**

Although you may originally have set your updates for viewing only by people you are connected to, some social media sites update their policies, and users don't realize they have to opt-out of some new public-view settings.



## **Only accept invitations to link online with people you know well in real life.**

Unless the information you share is very general, it's probably safer only to accept invitations to connect with people you know.



## **Don't display the names of the people in your network.**

While you may not be victimized directly, your connections might be. **Spear-phishing** scams rely on cybercriminals gathering enough personal information to send out convincing emails, seemingly from people known by the target. Access to the names of your connections may result in your friends getting bogus emails from somebody pretending to be you.



## **Post updates and event announcements that aren't super specific.**

Don't give out exact locations or times of your activities and events. Save any special event details for the private invitations you send to guests. Otherwise you'll be announcing when you aren't or won't be home—great information for would-be thieves. This tip is also important to remember when you're about to post from your vacation.



## **Share but don't over-share.**

Before making your updates online, take a moment to remember you should be cautious. Don't be guilty of TMI—too much information. The information you choose to share may be shared by your connections to their networks. Ultimately, once your information is on the Internet, you have no control over who may see it.

# Why to be wary of public Wi-Fi

Public Wi-Fi may be convenient but it's rarely safe. Hackers can "eavesdrop" on your unsecured connections and steal personal information, like passwords and credit card numbers. Learn how to stay secure on public Wi-Fi.

## Don't:

- Allow your device to auto-connect to Wi-Fi networks
- Leave your Wi-Fi or Bluetooth on if you are not using them
- Access websites that hold your sensitive information, such as financial or healthcare accounts
- Log onto a network that isn't password protected

## Do:

- Disable file-sharing
- Only visit sites using HTTPS
- Log out of accounts when done using them
- **Use a VPN.** Norton WiFi Privacy creates a virtual private network that encrypts all your information on public Wi-Fi, making your public connection private





## How to spot secured vs. unsecured Wi-Fi hotspots





# Protect your devices with top-rated security by Norton

Your new device deserves award-winning security.<sup>6</sup> But don't forget about all your older devices, which are equally vulnerable to online threats. Protect all your devices and experience a new sense of security with Norton products that regularly receive top marks in industry tests.


**Norton Security Standard** offers comprehensive protection for your PC or Mac. [Learn more](#) 


**Norton Security Deluxe** protects up to five devices, including PCs, Macs, and Androids and iOS devices, with real-time protection against existing and emerging threats. It safeguards against viruses, spyware, malware, and other online attacks. [Learn more](#) 


**Norton Security Premium** covers up to 10 devices, and adds protection for your important files and documents against threats such as hard-drive failures and ransomware. You can automatically back up and encrypt 25 GB of data from your PC to our secured cloud storage. [Learn more](#) 


**Norton WiFi Privacy** is a VPN app that secures any Wi-Fi connection by turning it into a virtual private network to encrypt all of the information entering and leaving your device. Norton WiFi Privacy prevents hackers from “eavesdropping” on your private information when you're using public Wi-Fi. [Learn more](#) 


**Norton Mobile Security** protects your Android and iOS smartphones and tablets against digital threats like risky apps, while also offering controls to guard your online privacy. If your mobile device is lost or stolen, Norton Mobile Security enables recovery, and lets you lock or wipe your device remotely. [Learn more](#) 

**Norton Safe Search** ensures that the sites you visit are safe and legitimate—not phishing or fraudulent. Conveniently free and always on, Norton Safe Search is a search environment developed with a focus on online safety. [Learn more](#) 

**Norton Safe Web** is a free website rating service that makes it easy to differentiate safe Internet websites from potentially malicious ones. Supporting Google, Yahoo, Bing, and Ask.com, and using the Norton Toolbar installed on your PC, Norton Safe Web lets you know how safe a particular website might be before you view it. [Learn more](#) 

**Norton Identity Safe** is a free password manager that makes logging on to your favorite sites easier and more secure. It keeps your passwords synchronized across different computers, browsers, and mobile devices, with your passwords stored in a secure cloud-based vault that only you can access. [Learn more](#) 

**Norton Family Premier** is parental control software that helps your kids explore, learn from, and enjoy their connected world safely. Know at a glance when and where your kids spend time online. [Learn more](#) 

**Norton Identity Protection Elite** safeguards the life you've built by providing extensive monitoring, alerts, and restoration services to keep your identity safe. If your identity is compromised, a U.S.-based team of identity restoration experts will work with you until the problem is resolved. [Learn more](#) 

For more ways to secure your devices: **“How to Set Up and Secure Your New Tech”**

Award-winning Security



Reprinted with permission.  
© 2017 Ziff Davis, Inc. All Rights Reserved.

# Stay in the know with Norton

For timely tips on how to protect your devices and other online security issues, read articles on the [Norton Protection Blog](#) and rapid response updates to the latest threats at [Security Covered by Norton](#).

## Follow Norton



## Share this eBook with your friends and family



© 2017 Symantec Corporation. All rights reserved. Symantec, the Symantec Logo, the Checkmark Logo, Norton, and Norton by Symantec, are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Microsoft and the Windows logo are trademarks of Microsoft Corporation in the United States and/or other countries. Google Chrome is a trademark of Google, Inc. Firefox is a trademark of Mozilla Foundation. Mac, iPhone and iPad are trademarks of Apple Inc. Other names may be trademarks of their respective owners.

<sup>1</sup> Norton, "Norton Cyber Security Insights Report 2016," October 2016. <https://us.norton.com/cyber-security-insights-2016>

<sup>2</sup> Ericsson, "North America Ericsson Mobility Report," November 2015. [www.ericsson.com/mobility-report](http://www.ericsson.com/mobility-report)

<sup>3</sup> Pew Research Center, "Spring 2015 Global Attitudes Survey," February 23, 2016. <http://www.pewglobal.org/2016/02/22/smartphone-ownership-and-internet-usage-continues-to-climb-in-emerging-economies/>

<sup>4</sup> Symantec, "Internet Security Threat Report 2016," April 2016. <https://www.symantec.com/security-center/threat-report>

<sup>5</sup> Statista, "Average daily time spent on social media worldwide 2012-2016," September 2016. <https://www.statista.com/statistics/433871/daily-social-media-usage-worldwide/>

<sup>6</sup> As of 2016, PC Magazine has awarded the Editors' Choice Award to Norton security products 39 times since 2001—more times than any competitor. Recent Editors' Choice Award winners include Norton Security Premium (awarded on August 25, 2016 and October 27, 2015) and Norton Family Premier (awarded on October 19, 2015).

