GOT A NEW PC OR MOBILE DEVICE?

Here's how to use it safely online.

Norton™ by Symantec

It's not just those who grew up with technology who appreciate what a digital life can offer. Technology has brought exciting changes to many of our daily activities—from shopping to navigating, banking to entertainment, communicating to learning, dating to eating, and so on. That's why today, the young, the old, and everyone in between seem to have at least one device connected to the Internet. In fact, the average U.S. household now owns 5.2 connected devices.[1]

The problem is that many of us are exposing our devices' rich information and activities to potential theft and fraud. How? By not securing our PCs, laptops, tablets, and smartphones the way we secure other parts of our lives. Cybercriminals are eager to take advantage of this gap. For instance, they are thrilled to know that so many people are using their PCs and mobile devices for activities such as banking and shopping and they aren't protecting their devices and information:

- One in three consumers do not have a password on their smartphone or desktop computer.[2]
- In the United States, more than one-third of those who have shared passwords have shared the password to their bank account.[3]

And it's not just online banking and shopping where there's danger. We also have to be careful and protect ourselves when using social media, email, mobile apps, and browsers. Read on to find out why.

As the number of mobile devices increases, so do the security threats

At **7.22 billion,** there are more mobile devices on the planet today than there are people.

The average app user has **36 apps** installed on his or her smartphone.

More than **1 million** malicious mobile apps are in existence.

17 percent of all Android apps (nearly 1 million) are actually malware in disguise.

Sources: *GSMA Intelligence, Google/Ipsos Survey, Symantec Internet Security Threat Report*

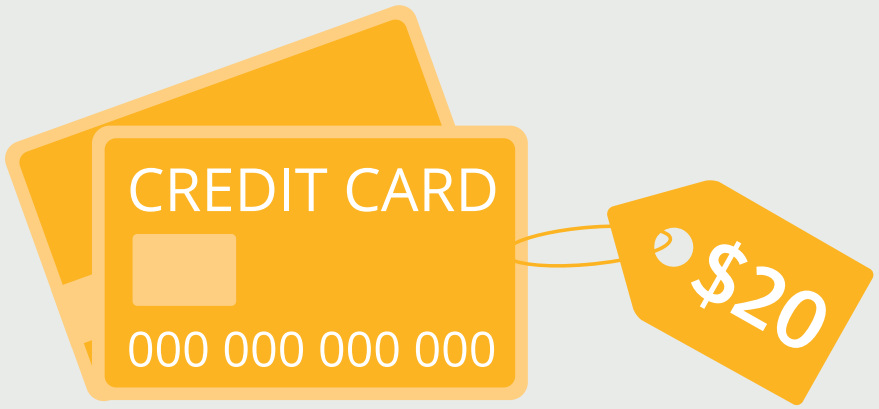
[1] "North America Ericsson Mobility Report," *Ericsson* (November 2015), www.ericsson.com/mobility-report.

[2] "Norton Cybersecurity Insights Report," *Norton* (November 2015), http://us.norton.com/cyber-security-insights.

[3] Ibid.

Don’t let your information end up on the black market

Cybercriminals will always choose the easiest targets to steal: personal information, passwords, bank account numbers, credit card information, contacts, and other data they can use or sell. Often they target your mobile device or PC. Did you know that your credit card details are worth as much as $20 on the black market? Stolen gaming accounts can garner nearly $15 for cybercriminals.[4]



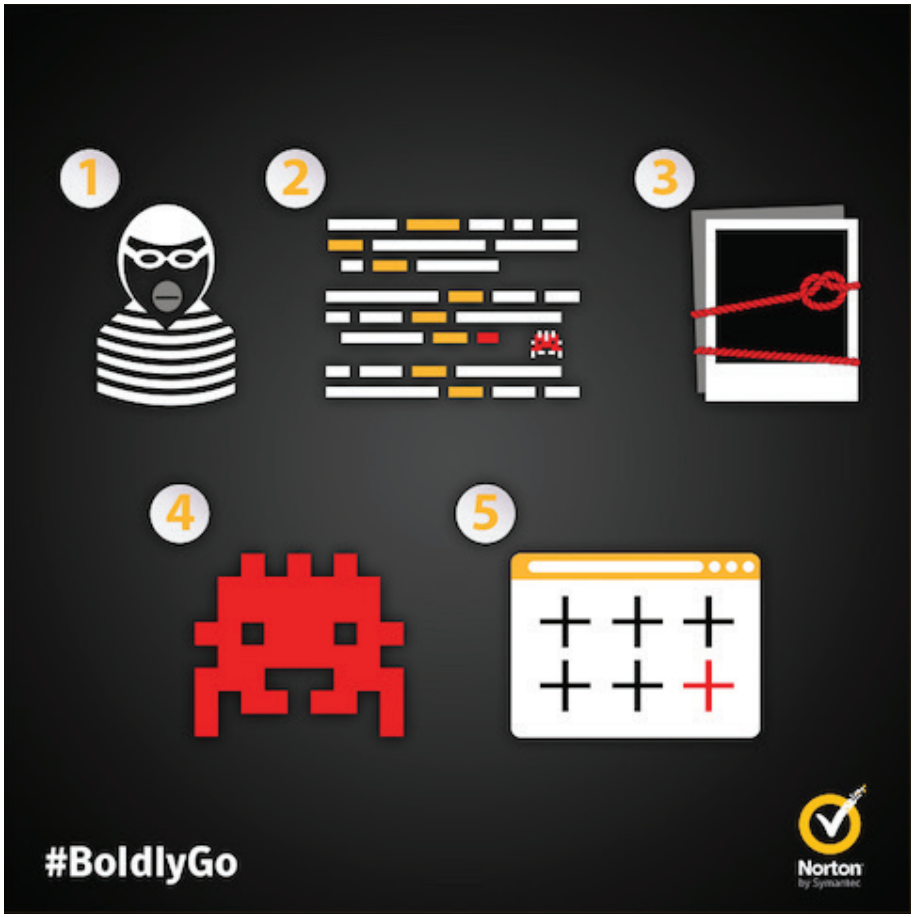
[4] “Internet Security Threat Report, Volume 20,” *Symantec* (April 2015).

Top online threats for consumers

Hacker Method	How It Works	Devices Impacted
Malware	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.	**Every device that can connect to the Internet**
Ransomware/ crypto-ransomware	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.	**Mostly PCs, laptops, notebooks, but also mobile devices**
Phishing	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.	**Every device connected to the Internet**
SMiShing	SMiShing is phishing using text messaging (SMS) and other mobile messaging technologies to deliver all kinds of scam campaigns. Top categories in 2014 for SMS spam/scams included adult content, payday loans, account number phishing, rogue pharmacy scams, and others.[5]	**Mobile phones**
Social media	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 a piece of music, or enter a competition. Users are often asked to give their account login information or text a premium rate number.	**Every device connected to the Internet**
Identity theft	Criminals use phishing scams to get you to divulge personal information to steal your identity. Lost or stolen devices, or disposing of old devices without wiping them clean, can also provide thieves with what they need.	**Every device connected to the Internet**
Fake networks	Hackers can exploit open Wi-Fi networks to intercept email messages, passwords, login credentials, or other information sent to unsecured sites. Some can even set up fake hotspots to read the wireless traffic flowing over them. These networks often have generic names such as “airport” or “free Wi-Fi.”	**Mobile devices you use outside of your home, such as laptops, notebooks, tablets, and smartphones**

[5] “Internet Security Threat Report, Volume 20,” *Symantec* (April 2015).

Want to learn more about online security threats? Read our article, 5 Ways You Didn't Know You Could Get a Virus, Malware, or Your Social Account Hacked.



Did you know? Malware apps can

- Track your device's location.
- Use audio and video to monitor your activities.
- Divert texts from your bank.
- Make charges to your phone.
- Message your contacts.
- Collect device information.
- Download and install apps and files.
- Hand over control of your device to an attacker.

Use these seven tips to protect your PC, laptop, and mobile devices

1. **Install comprehensive security software:** Choose a software package that protects you against malware, ransomware, and phishing scams and lets you back up and restore your files. In addition, look for software that can remotely lock and wipe mobile devices if they are stolen or lost.

2. **Back up your data:** Make it a habit to regularly back up your PC, laptop, tablet, or smartphone to the cloud or portable storage device. Otherwise, if your device is damaged, lost, or stolen, your contact numbers, treasured photos and videos, and important financial and work documents might be lost along with your device.

3. **Be a savvy online shopper:** Make sure you don't pick up malware along with your bargains, and don't be fooled into giving your personal details away.

4. **Protect your personal information:** Transact financial business online only with secure websites. Make sure URLs begin with HTTPS. Avoid phishing scams—use caution when clicking links in email, social media, or texts. Be careful about what personal information you divulge on social media sites. Never send personal information such as credit card numbers via email, text, or instant message or across social networks.

5. **Lock your device and SIM card with a PIN/password:** Prevent others from accessing your online accounts or other private information by locking your device. Ensure your password is memorable—and strong—at least eight characters, including uppercase and lowercase letters, numbers, and symbols.

6. **Be careful with apps:** Read the reviews. Download only from reputable app stores, such as Google Play, Apple App Store, or Windows Phone Store. You might be tempted to load your mobile devices with all the latest entertaining apps, but first stop and think—is it safe?

7. **Disable Wi-Fi, Bluetooth, and geotagging:** Stop 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 geotagging feature, which identifies the location where photos are taken, allowing someone else to track your movements if the photos are published online.

For more ways to secure your devices, read this article:

Giving someone a hand-me-down PC or device? Follow these steps

1. Restore the device to factory settings if it is a mobile phone or tablet, or erase the hard drive if it is a PC or laptop by installing a clean version of the operating system.
2. Clean the device of any content, including personal files, passwords, and credit card information, before handing over to others.
3. Delete your browser history and cookies and review applications.
4. Verify that cloud storage settings on the device are correct, or change them.

Protect your devices with top-rated security software

Symantec's Norton™ security products are top-rated in comparative tests by independent entities.[6] Find the right solution for your needs:

Norton Security Standard offers comprehensive protection for your PC or Mac. **Find out more**

Norton Security Deluxe protects up to five devices, including PC, Mac, Android, and iOS devices (some features not available on iPad and iPhone), with real-time protection against existing and emerging threats. It safeguards against viruses, spyware, malware, and other online attacks. **Find out more**

Norton Security Premium adds protection of 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. **Find out more**

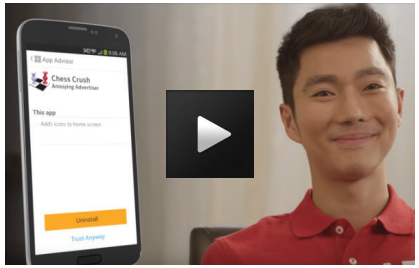
Norton Safe Search ensures that the sites you visit are safe and legitimate—not phishing or fraudulent. Conveniently available and always on, Norton Safe Search is a search environment developed with a focus on online safety. **Find out more**

Norton Safe Web is a 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. **Find out more**

Norton Identity Safe is a free password manager that makes logging into 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. **Find out more**

Norton Family is parental control software that helps your kids explore, learn from, and enjoy their connected world safely. **Find out more**

Learn more about how Norton can protect your device from risky apps.
Watch the video



Award-winning security

PC EDITORS' CHOICE
PCMAG.COM
34 TIME WINNER

Norton Security is 34-time winner of the PC Magazine Editors' Choice Award.

[6] "2015 Consumer Security Products Performance Benchmarks," *Passmark Software* (March 2015), www.passmark.com/ftp/totalsecuritysuites-mar2015.pdf.
"PC Anti-Malware Protection 2015," *Dennis Technology Labs* (September 2014), www.dennistechnologylabs.com/av-protection2015.pdf.
"Product Review and Certification Report," *AV-Test* (December 2014), www.av-test.org/en/antivirus/home-windows/windows-7/december-2014/norton-norton-security-2015-144948/.

Consider the advantages of paying for protection

Would you buy a car without insuring it? How about that expensive bike? It's covered under your home insurance plan, isn't it? We routinely pay to protect ourselves against loss, damage, or theft for things that are valuable to us.

Today, those things include our PCs and devices, our confidential information, and the safety and security of our families. To protect your PCs and devices, you have two choices: Either install a free security solution or purchase a subscription-based security solution.

Free isn't always free

Opting for a free solution can be tempting. However, when you think about private information, sensitive transactions, and irreplaceable photos and files that reside on your devices, would you trust a free solution to protect you when so much is at stake? While free antivirus may help protect you against viruses, it probably won't help protect you against other dangerous online threats.

The right protection isn't expensive

For less than it costs to download a new tune or stream a movie, you can get the right protection for each of your devices.[7]

[7] $1.34 per device per month; price based on Norton Security 12-month subscription, activated on five devices. Simulation based on Norton Security Deluxe for five devices. Norton Security is a subscription-based service billed once a year or every two years, depending on selected product offering and length.

Freeware limitations

Less comprehensive: Free Internet security software offerings may have less comprehensive monitoring of system behaviors and therefore be less likely to identify and respond to new and evolving threats.

No guarantees: Freeware usually doesn't come with an additional protection guarantee or promise.

Basic level of protection: Free Internet security software usually offers only a basic level of protection, such as scanning for malware and viruses. In fact, recognizing that free security software doesn't offer complete coverage, companies offering freeware frequently recommend their paid versions.

Paid security protection benefits

Better threat protection: Norton Security offers comprehensive protection against existing and emerging threats to your devices and your personal information.

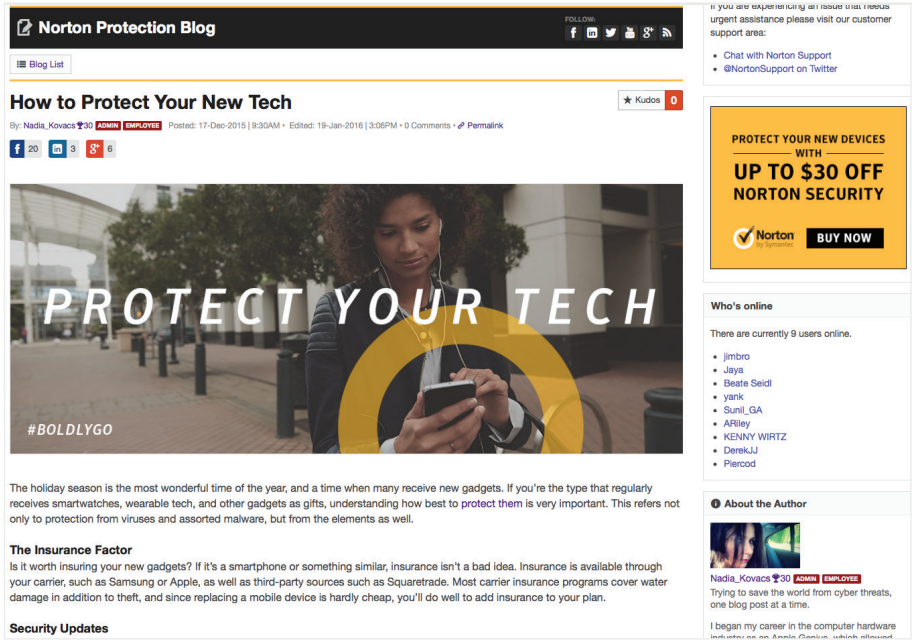
Virus Protection Promise: Norton Security gives you support when you need it, with online or phone access to an expert Norton technician. And it comes with our Virus Protection Promise: If any of your devices gets a virus that Norton cannot remove, we'll give you a refund.[8]

Comprehensive package: Norton Security offers a simple, single solution to meet your family's security needs including parental controls, firewalls, system performance tools, identity theft protection, anti-spam measures, password and login protection, and more.

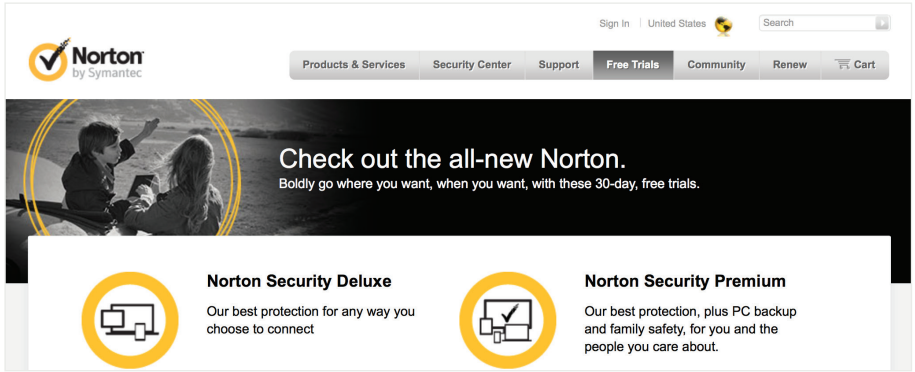
[8] To be eligible, you must purchase or renew your Norton subscription directly from Symantec or from a retail store and subscribe to the Norton Automatic Renewal Service online. If a Symantec service representative is unable to remove a virus from your device, you may receive a full refund on the actual price paid for the Norton subscription, or, if a bundle, the total price of the bundled price paid (net of any discounts or refunds received and less any shipping, handling, and applicable taxes, except in certain states and countries where shipping, handling, and taxes are refundable) and only for the current paid subscription service period for that product or product bundle. The Norton subscription must be installed and activated on your device prior to the time it is infected by a virus. The refund does not apply to any damages incurred as a result of viruses. See Norton.com/guarantee for details.

Take the next step

Stay up-to-date on how to protect your devices by reading our Norton Community blog.



Try Norton Security for yourself. Download your free 30-day test version.



Share this eBook with your friends and family.