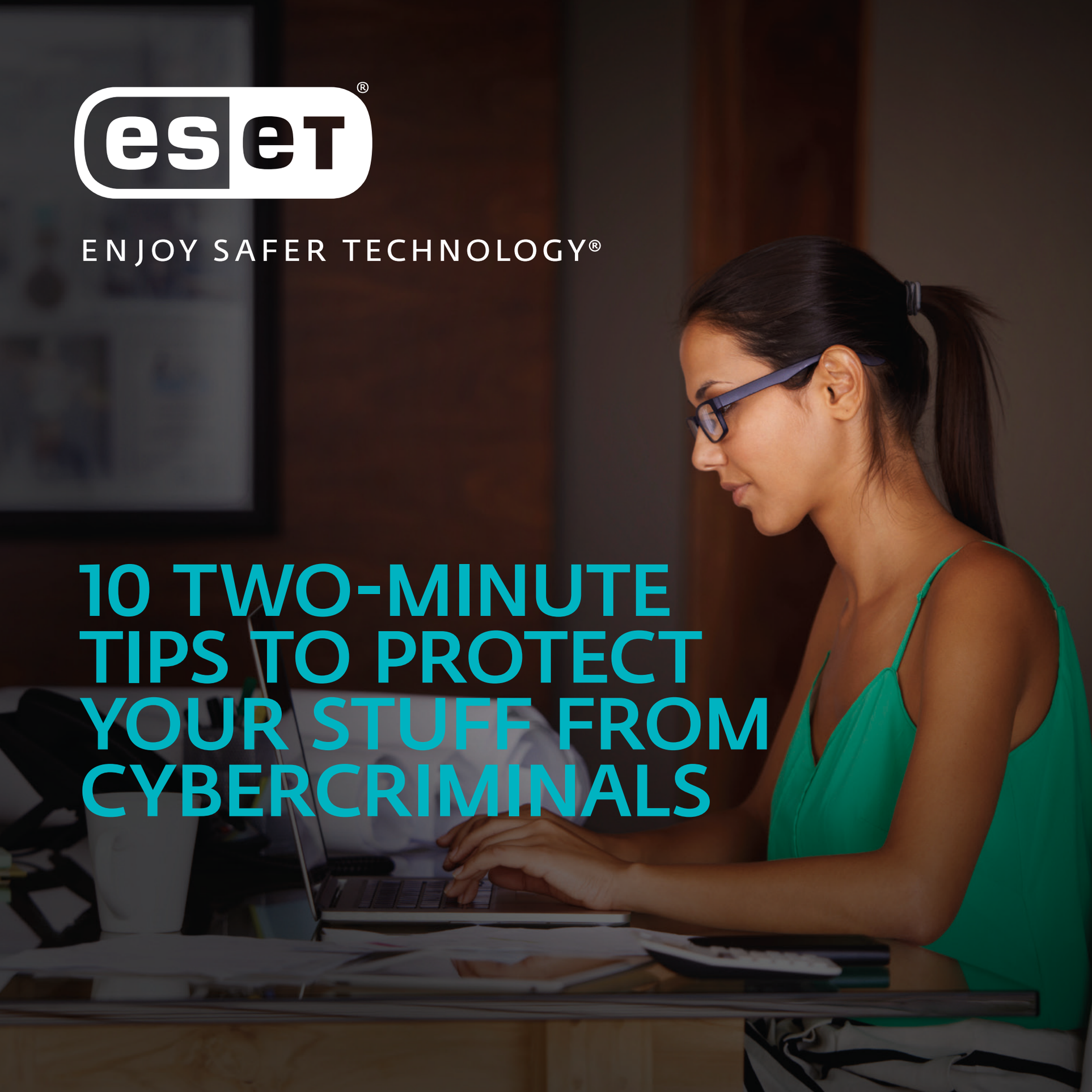
ENJOY SAFER TECHNOLOGY®

10 TWO-MINUTE TIPS TO PROTECT YOUR STUFF FROM CYBERCRIMINALS



10 two-minute tips to protect your stuff from cybercriminals

Performing a "cybercleaning" might sound time-consuming—but you can complete many security fixes in two minutes or less.

Whether it's a PIN you thought up in a rush—one a cybercriminal could guess just as easily—or a security option you forgot to switch on, don't leave any door open to hackers and scams. Here are 10 quick fixes that can make you safer.

1. Is your smartphone PIN easy to remember? Change it!

A huge percentage of smartphone users still choose obvious PIN codes such as 1234 or 1111. Criminals will try these chestnuts, and will make every other effort they can think of to guess your PIN—sometimes even assisted by the telltale cluster of your finger marks on a device screen. Remember, all the data in your mobile device is available to any criminal who gets hold of your PIN—and that can include everything from the data in your email account to online banking passwords.

2. Don't "opt out" of security: Tick the box to choose two-factor authentication on Twitter, Gmail and Dropbox.

Two-factor authentication makes it far more difficult for cybercriminals to break into accounts on sites such as Google and Twitter. At present, though, two-factor authentication is "opt-in"—you have to go to Settings and choose this method manually. With Gmail, for example, you can access Google's two-step verification process from your Account Settings page, under the "Sign in and Security" section. Then follow the steps to complete the process.

3. Get rid of passwords that end with numbers and "!"

Many sites force users to replace passwords occasionally—and users often respond by simply adding the required special characters or numbers to the end of their existing passwords. These are among the first variations a would-be password cracker will try. To be safer, place numbers or special characters in the middle of a password, and avoid the commonest symbols—especially "!"—altogether.

4. Check that you don't have viruses right now.

Free antivirus software—or instant checks—can't ever match the peace of mind you get from having a proven security solution installed on your computer and protecting you 24/7. But if you're worried you may have clicked the wrong link, or something just seems wrong, **ESET's Online Scanner** can perform an instant scan of your PC for free.

5. Be careful when using public Wi-Fi.

Free Wi-Fi networks can offer a convenient and no-cost way to get online. But use caution: Always ask the owner of the Wi-Fi hotspot for the correct network name and password. Be wary if there is no WPA or WPA2 password (for Wi-Fi protected access), as this will mean the connection is unencrypted—and pay close attention to potentially spoofed hotspots that bear close resemblance to the spot's real name.

Remember, it's far more secure to use your smartphone's data connection and share it with your laptop via Wi-Fi. It's very difficult to tell whether data is being intercepted on open public networks—and if you use such networks to access sites where you have to enter a password to reach your data (such as Web email or online banking sites), you're at very real risk of being hacked. Don't take that risk.

6. Keep your mobile phone and apps up to date.

Mobile devices are every bit as vulnerable to security hacks as laptops and PCs. Having the most up-to-date security software, Web browser, operating system and apps is the best defense against viruses, malware and other online threats. Try to avoid postponing updates.

7. Watch what you click.

Cybercriminals will seize any opportunity to get someone to click a link that takes him or her to a bad website. This is especially true around major events, like natural disasters or the Olympics—the numbers of spam emails, tweets and more simply skyrocket. If you see a link for something about a major earthquake or celebrity scandal, take a moment. Think again about the source of the link, where it has been shared and where the link is taking you. Is it really worth clicking?

8. Back up everything.

We've said it before: Get into the habit of backing up your data regularly. We recommend doing it at least once a week. Not only will taking this precaution protect you in the event your laptop is stolen or your hard disk fails, but it also gives you more options for recovery if your computer gets infected with ransomware. (Ransomware encrypts your files and threatens to delete them if you don't pay a ransom within a certain time period. **Read more** about ransomware.)

ESET doesn't recommend giving in to **ransomware** demands for many reasons (not least because you mark yourself as a possible target for future attacks), but if your files are all safely backed up, you won't even feel tempted to negotiate with the data-nappers in the first place. Backup methods include external hard drives, cloud solutions (such as Dropbox) and USB drives (such as the **Kingston DTVP 3.0 USB Flash drive with DriveSecurity by ESET**).

9. Change default passwords on everything.

Many security cameras, baby monitors and some webcams operate independently of your PC—and therefore independently of the security protection offered by PCs and good antivirus software. If these devices are not secured properly, anyone could potentially access them through a website or app.

What makes these devices vulnerable is that they all make use of a preconfigured "default password" during their set-up process. ESET Security Specialist Mark James says that a device connected to your system is relatively easy for a cybercriminal to find using specialized search

engines—and that the URL used to log in and the default password for that device can easily be found online. If you've taken the extra precaution of changing this default password, you can stop a straightforward security incursion through that channel right in its tracks.

To learn how to change the default password for any device, simply check the user manual or manufacturer website for instructions. Here are more easy ways to improve your security at home that you might not have thought of.

10. Opt for more privacy on Facebook.

Have you checked your privacy controls recently? With more than one billion users on Facebook, there are plenty of cybercriminals out there hoping to steal data from legitimate users. Here's a tip adapted from the social media watchdog site **Facecrooks**:

Facebook gives you the ability to control who sees your Friends list. We recommend setting this feature to "Only Me." When cybercriminals hijack a Facebook account, they tend to extract as much data as possible. This information can be used to commit fraud and identity theft, and to find more victims. Leaving your friends list open to "Friends" can expose all of your Facebook friends to hackers and scammers.

If the scammer doesn't know who you're friends with, then it's virtually impossible for him or her to run this socially engineered scam successfully.

Here's how to lock down your Friends list:

- Navigate to your Timeline and click the link to your Friends list.
- Next, click the "Edit Privacy" icon located on the far right, and set the Friends list option to "Only Me."

For over 25 years, ESET® has been developing industry-leading security software for businesses and consumers worldwide. With security solutions ranging from endpoint and mobile defense to encryption and two-factor authentication, ESET's high-performing, easy-to-use products give users and businesses the peace of mind to enjoy the full potential of their technology. ESET unobtrusively protects and monitors 24/7, updating defenses in real time to keep users safe and businesses running uninterrupted. For more information, visit ***www.eset.com****.*

ENJOY SAFER TECHNOLOGY®