THE 5 THINGS YOU NEED TO DO TO PROTECT YOURSELF FROM RANSOMWARE

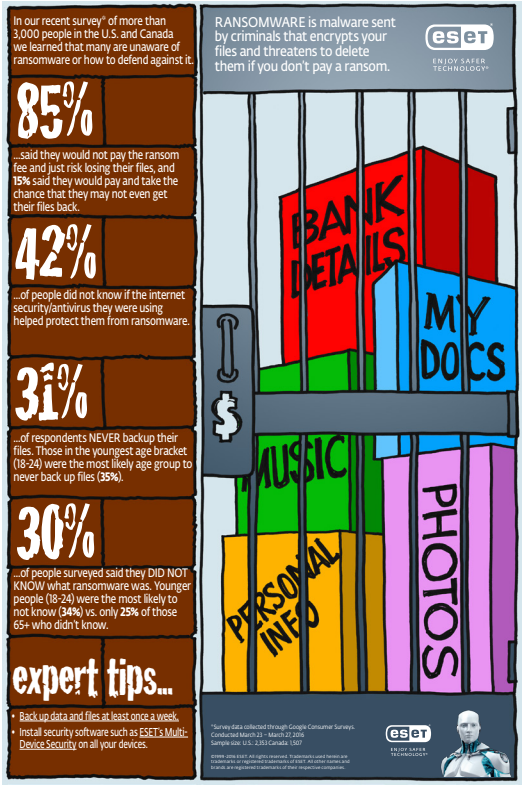
The 5 things you need to do to protect yourself from ransomware

By Stephen Cobb, ESET Senior Security Researcher

Family photos and videos. Tax returns and other financial records. Business documents. Think about everything that you keep on your computer. What would happen if it all was stolen from you?

That's what a ransomware attack does. Criminals use this nasty breed of software to reach out over your internet connection and kidnap the contents of your computer, literally holding them for ransom. Ransomware silently encrypts all of your personal files, making them unreadable, and then demands that you send money to the criminal in order to restore them.

We surveyed over 3,000 people across the U.S. and Canada to understand what knowledge everyday people have about ransomware and we learned some surprising information. Despite the widespread reporting of ransomware in the news in recent months, many people still don't know what ransomware is. Even fewer people take the steps necessary to protect their data from a ransomware attack. Below are the results—and how to protect yourself.



Fortunately, protecting yourself is easier than you think. Ransomware authors use strong encryption techniques to lock up your files and only the kidnapper has the key. These criminals typically offer only one way out: pay the ransom, or kiss your data good-bye. And, even if you do pay, there's no guarantee you'll get the key to get your files back. Despite the repercussions, many people are unaware of ransomware or how to defend against it, as our new survey shows.

Hopefully you will never be forced into that situation, and with these tips you can prevent ransomware from holding your digital life hostage.

1 **Keep your software programs up-to-date.** Update your operating system and software with the latest patches and updates. Enable automatic updates if you can. (All those pop-ups can be annoying, yes, but there is a good reason for them–they are often intended to protect you from hackers getting to your device through their software!)

2 **Install an internet security suite.** Install a full-featured security suite, such as *ESET Smart Security*, that provides comprehensive protection—not just antivirus. Look for the following:

- *Antispam that filters out emails that might contain ransomware-spreading attachments or links to ransomware-laden websites.*
- *Anti-Phishing that prevents you from visiting suspicious sites masquerading as trustworthy ones.*
- *An exploit blocker that protects against security holes in software often used to spread infections and adds another layer of protection by fortifying applications on users' systems that are often exploited, such as web browsers, PDF readers, email clients or MS Office components.*
- *Software firewall can block ransomware from connecting to a Command-and-Control sever before encrypting your files, providing an additional layer of defense.*

3 **Learn to spot a "phish."** Phishing schemes use various means to trick you, and are one of the most-common ways that data-nappers plant ransomware on your machine. One trick is to masquerade as an email from a well-known company, designed to look like the real thing. *Take this quiz* and see how well you can spot a phish (Internet Explorer has issues with this quiz; we recommend using another browser.)

4 **Back up your data.** The single biggest thing you can do to foil a ransomware attack is to keep a regularly updated backup of the files that are important to you. You can do this with an external drive, a

cloud backup service, or both. Bear in mind that ransomware will try to encrypt not just the files on your internal hard drive, but *also on any USB drives*, external drives or cloud-file storage that has been assigned a drive letter. So it's important that any backup service is either not assigned a drive letter or, disconnected when not actively doing a backup.

5 **Tweak your settings.** If you're an advanced user, there are some settings in your system that you can tweak to foil the current generation of ransomware. Check out our *We Live Security blog post* devoted to the subject, written by ESET security researchers.

It doesn't take much for ransomware to take over an unprotected computer. And while the possibility of an infection is alarming, an alarm can be a good thing. There are many, many ways you can lose your data. Ransomware is just one of them. But the steps you take to defeat ransomware will protect you against many other cyber threats. The first step in protection is awareness, so you now have the first one checked off your list! And remember. Back up, back up, back up... frequently! It has always been, and always will be, the best practice to protect your digital life.

Stephen Cobb has been researching information assurance and data privacy for more than 20 years, advising government agencies and some of the world's largest companies on information security strategy. Cobb also co-founded two successful IT security firms that were acquired by publicly traded companies and is the author of several books and hundreds of articles on information assurance. He has been a Certified Information System Security Professional since 1996 and is based in San Diego as part of the ESET global research team.

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®