Eldar Kudinov • Michail Diakov • Vasily Yaltonsky • Dennis Fisher

SURVIVING THE DIGITAL WORLD

Practical advice for keeping your online life secure

KASPERSKY lab

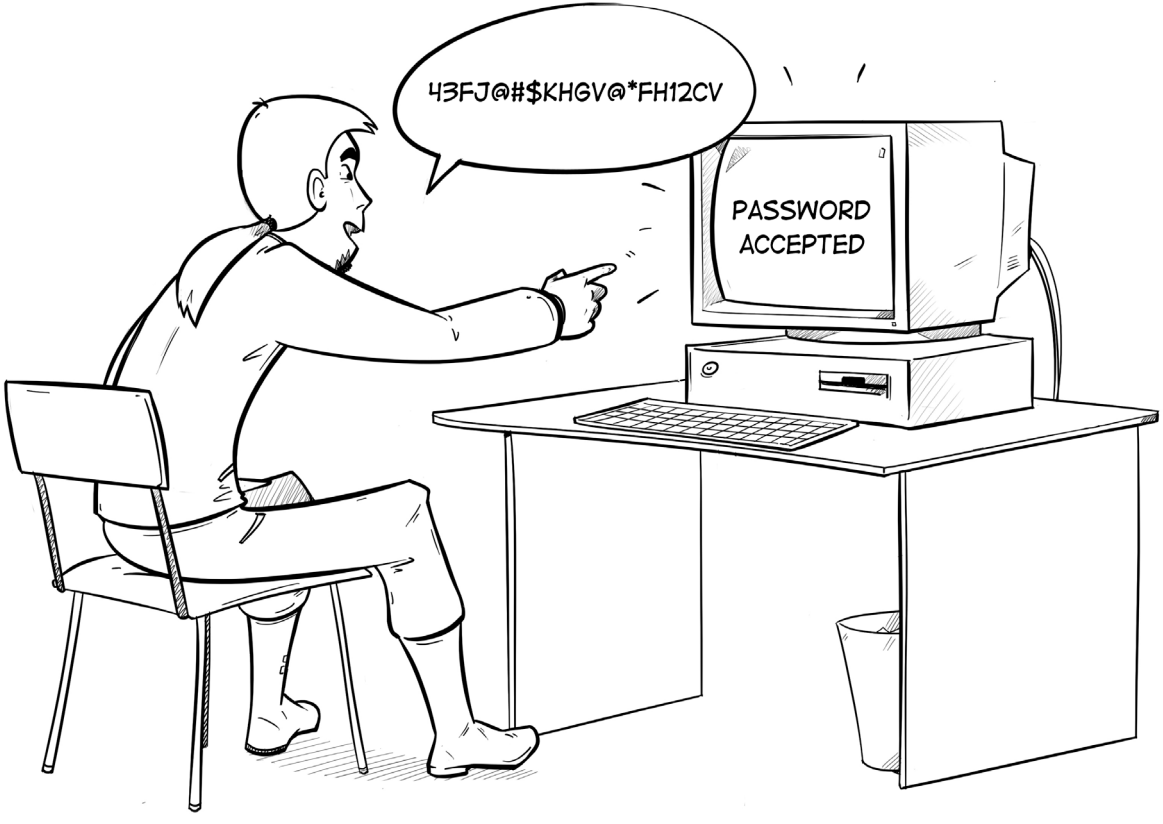
INTRODUCTION

The dawn of the digital age does not look like what we expected. PCs and mobile phones have given people access to vast amounts of knowledge and endless new ways to share it; our lives are easier and better thanks to new technology and the Internet. However, all of this good also came with a negative side full of personal information theft, malware, and groups of criminals who use the Web as their personal playground.

The good news is that there are people who are fighting this chaos and are willing to share their experience and knowledge with the next generation. So the dark part of the legend ends and our story begins...

TIP 1: **USEFUL INFORMATION**

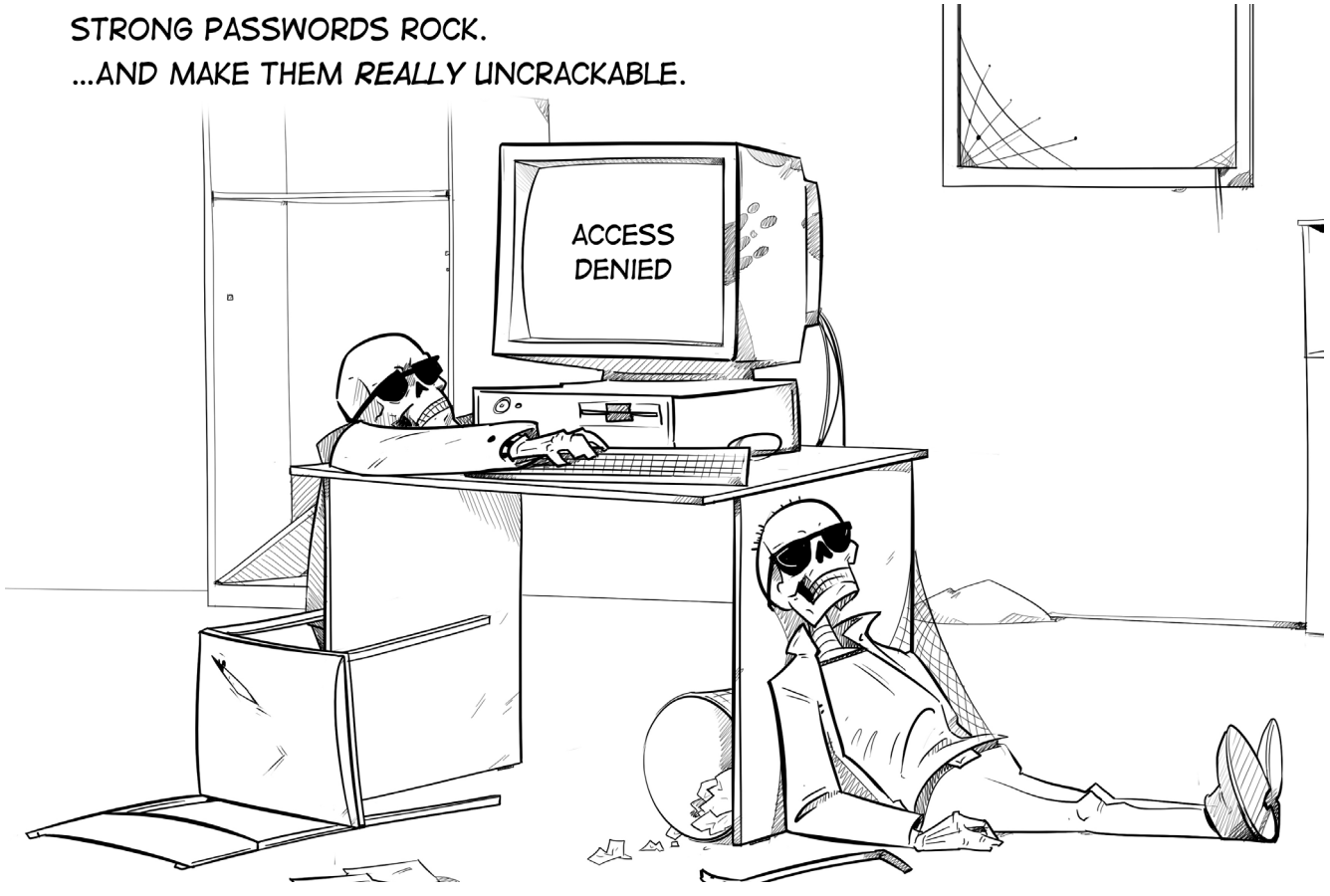
Just imagine: a virus infiltrates your computer via the telephone network, turns it on in the middle of the night and sends a command to launch a missile. It's a Hollywood scenario but in the real world, malware usually functions in a very different way and has a different purpose. The vulnerability of computer systems and the fact that users don't know the basic principles of information security are the key ingredients for the success of any piece of malware. It may sound incredible, but a hacker doesn't need to type a lot of strange information while scary music plays in the background if he wants to infect your computer. A single email with a malicious file enclosed is sufficient. If the victim believes the message is legitimate, she will start the malicious app herself. So in order to defend against cybercriminals, you must understand what the threats are.



BE *REALLY* CREATIVE WHEN CREATING PASSWORDS...

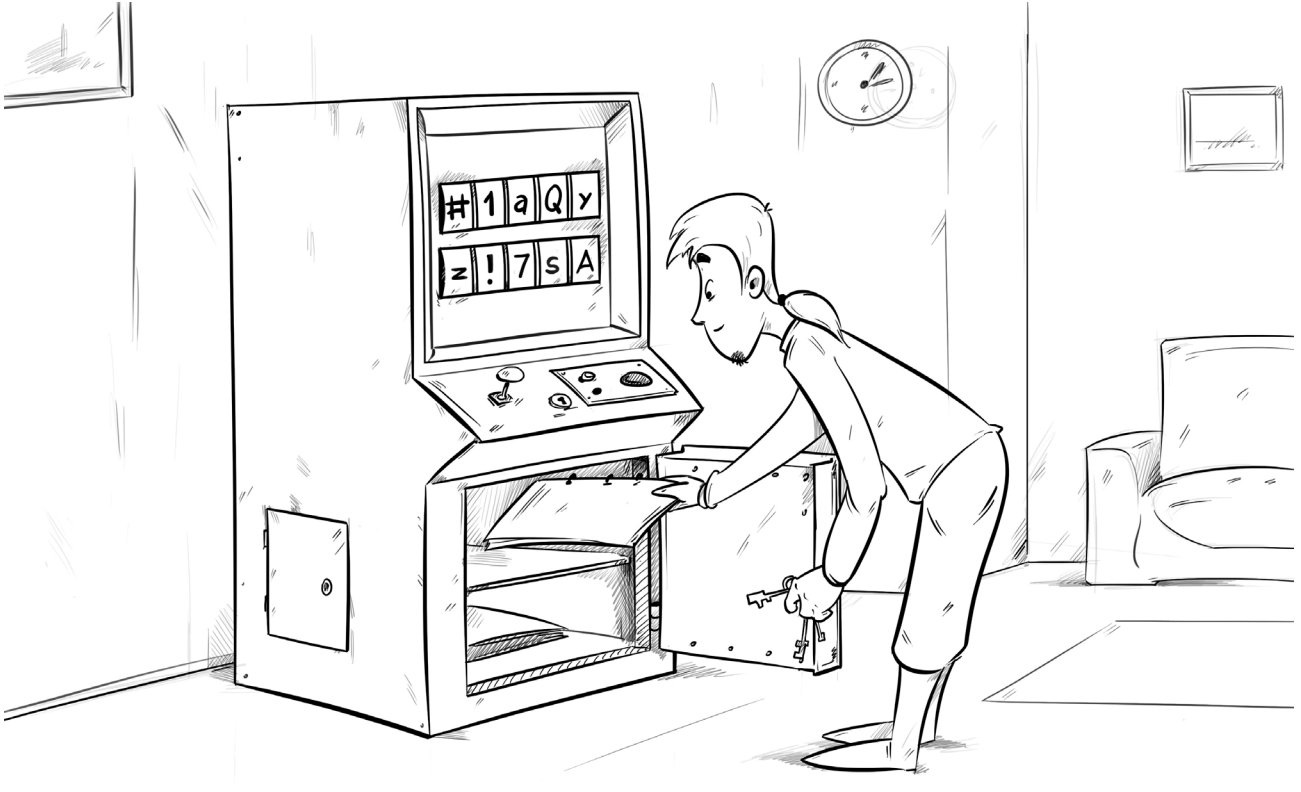
TIP 2: **PASSWORD STRENGTH**

Hackers usually start their work with a special vocabulary that contains millions of passwords that were previously used or leaked online. There are several people on this planet who think exactly like you, so your password may be on that list. You shouldn't use common words, song lyrics, a film title, your cat's name, your date of birth or any type of information that can be easily guessed or found on social media as a password.


STRONG PASSWORDS ROCK.
...AND MAKE THEM *REALLY* UNCRACKABLE.
ACCESS
DENIED

TIP 3: **A STRONG PASSWORD**

Associations are the easiest way to create a difficult password. Take a phrase associated with the service or website that you're signing up for, type it, add some numbers and letters. Now that is a strong password. Such a password is easy to remember and makes sense only to you.

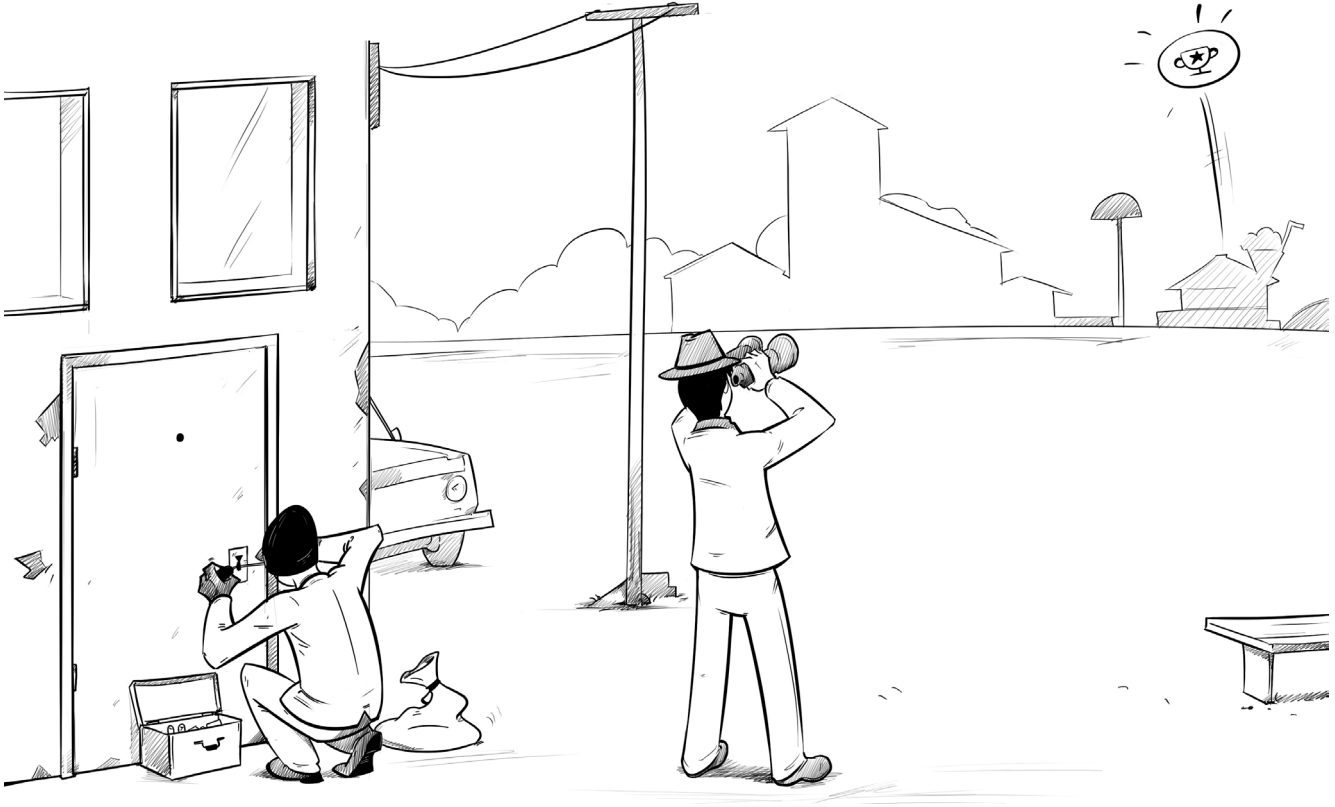


USE A PASSWORD MANAGER TO STORE YOUR PASSWORDS, NOT A STICKY NOTE.

TIP 4: **PASSWORD STORAGE**

The more difficult the password, the harder it will be to guess. The easier the password, the easier it is to remember. So it should be both difficult and easy – not everyone is capable of coming up with a good one. If TIP 3 doesn't suit you, then use a special password manager app. These apps will create difficult, unique passwords for on-line services, social media, applications etc., and then save them in its coded database. The only thing left for you is to create one main password for the manager. Remember: the password should be difficult so no one can guess it, and it's easy to remember!

DID YOU KNOW THAT YOUR CHECK-IN AT THE CAFE WASN'T PRIVATE?



TIP 5: **VIRTUAL SPYING**

In the past criminals would remotely view you, your apartment, country house or car. But all this is not all that interesting and out of date. Today's thieves can just subscribe to your news in the social media to find out where you are and where you are not should you make it a habit to check-in everywhere. Think about how many real and old friends there are in your Swarm or Facebook account the next time you check-in.


OVERSHARING OF YOUR PERSONAL BELONGINGS CAN LEAD TO THEFT.
1200 $
340 $
2700 $

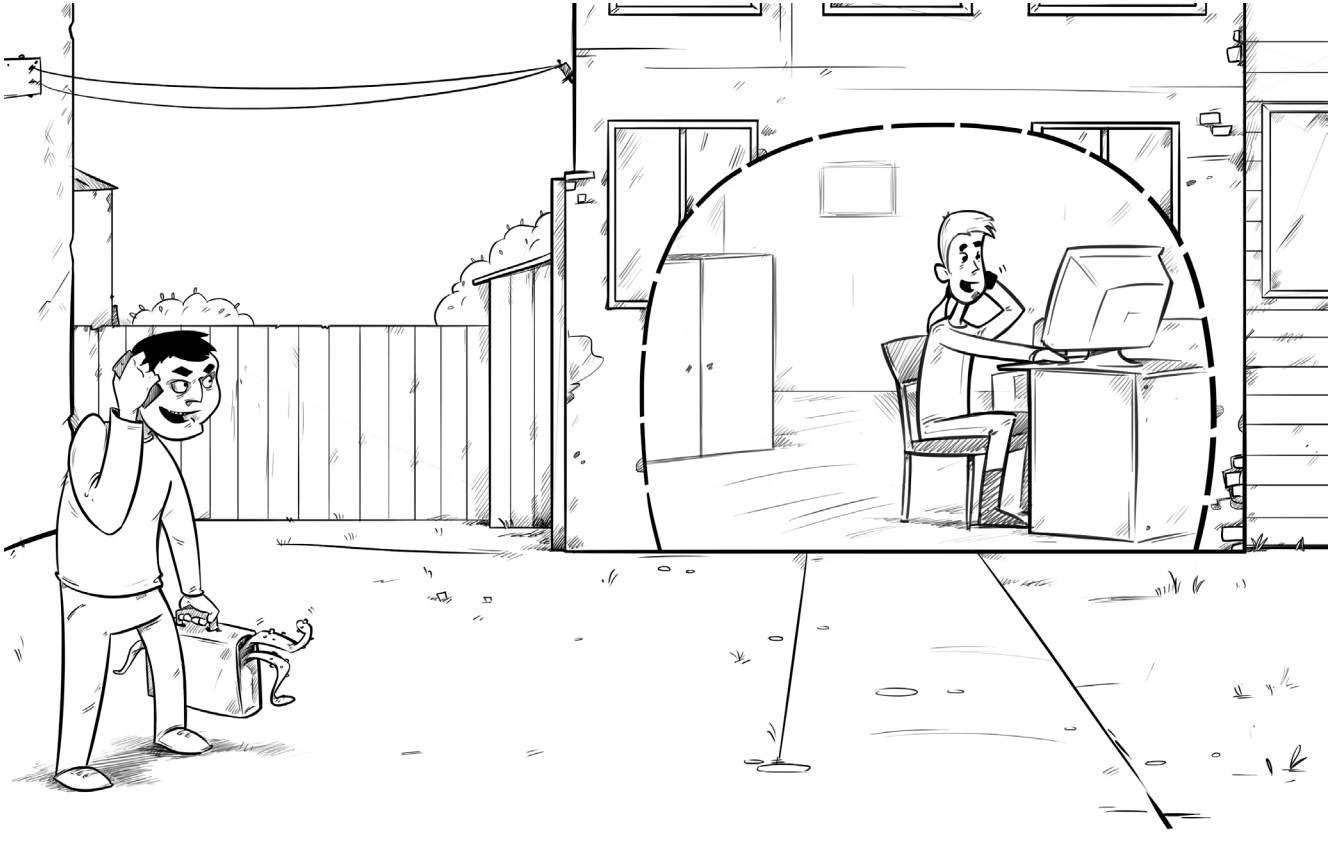
TIP 6: **BEAUTIFUL LIFE**

Criminals can use social media as well as we can and maybe even better because such skills are really useful in making them profit. You should be more modest in the virtual life for your own safety as photos of you luxury condo, new car or expensive laptop on the Internet or information that you'll be on vacation with a loved one next week could make you a target.

YOUR WEBCAM MIGHT BE USED TO SPY ON YOU.

TIP 7: **UNNOTISABLE SPY**

Web-cameras are perfect for people whose friends or relatives live far away. But, please, be sure that your cameras won't show the trespassers you private life. Hackers can use them in different ways. It all depends upon the fantasy and the story he or she has. They can sell photos and video to a porn site or blackmail the user. If you don't want such trouble to happen to you then use anti-virus app protection that will control the access to your camera.



A WINDOWS SUPPORT MANAGER IS A POPULAR CHARACTER USED BY FRAUDSTERS.

TIP 8: **TELEPHONE FRAUD**

“Hello, I am a specialist from Windows Technical Support. There is a very dangerous virus on your computer,” — this is a possible beginning of a talk with a telephone scammer. Everything is easy now: the trespasser convinces the user that his or her computer is infected and then recommends to do some actions that will certainly help. But the real malware is the very actions that are “recommended” by “the specialist.” So remember once and forever: Microsoft Technical Support won’t call you no matter how many viruses there are on your computer.