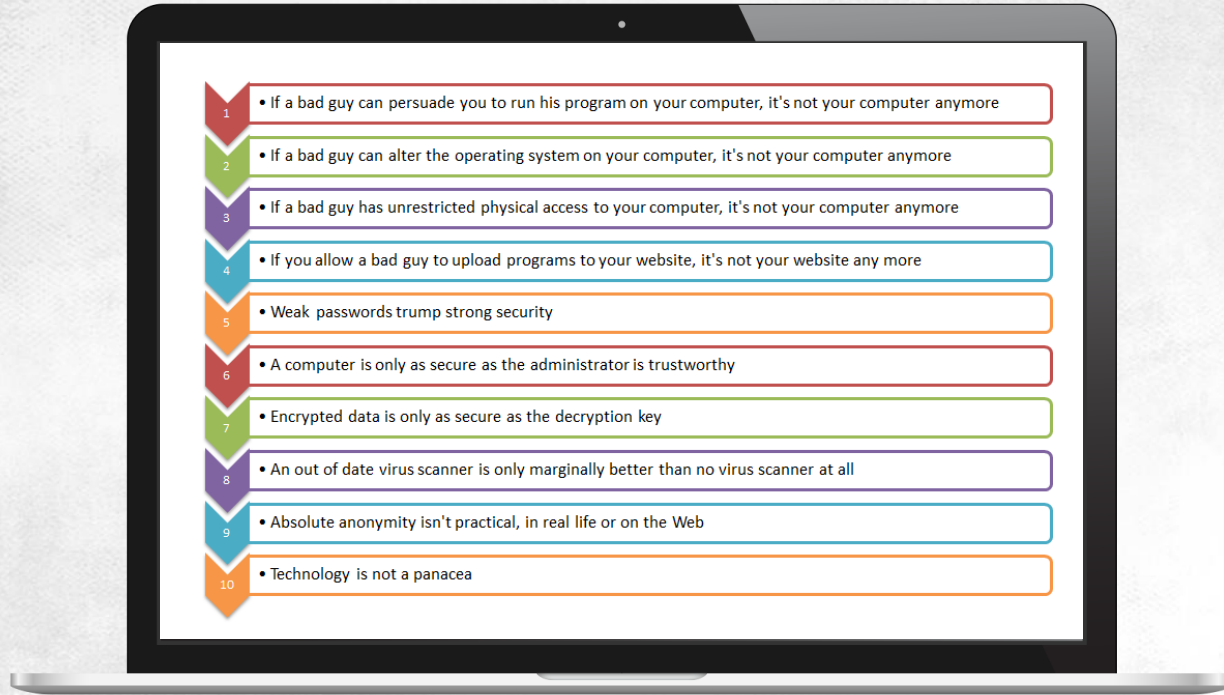


IMMUTABLE LAWS OF SECURITY



IMMUTABLE LAWS OF SECURITY

Developed in 2000 by Microsoft Security Response Center's Scott Culp, the Ten Immutable Laws of Security Pertain to computer systems. There is another version of these laws relating to administration security practices



IMMUTABLE LAWS OF SECURITY

Law #1. If a bad guy can persuade you to run his program on your computer, it's not solely your computer anymore

WHEN YOU RUN a program, you have no way of making sure it will only execute safe operations. In other words, once a program is started, you give up the control over it: operating systems have less security boundaries than you might have thought

THE ONLY WAY to mitigate this risk is running only the programs you fully trust



IMMUTABLE LAWS OF SECURITY

Law #1. If a bad guy can persuade you to run his program on your computer, it's not solely your computer anymore

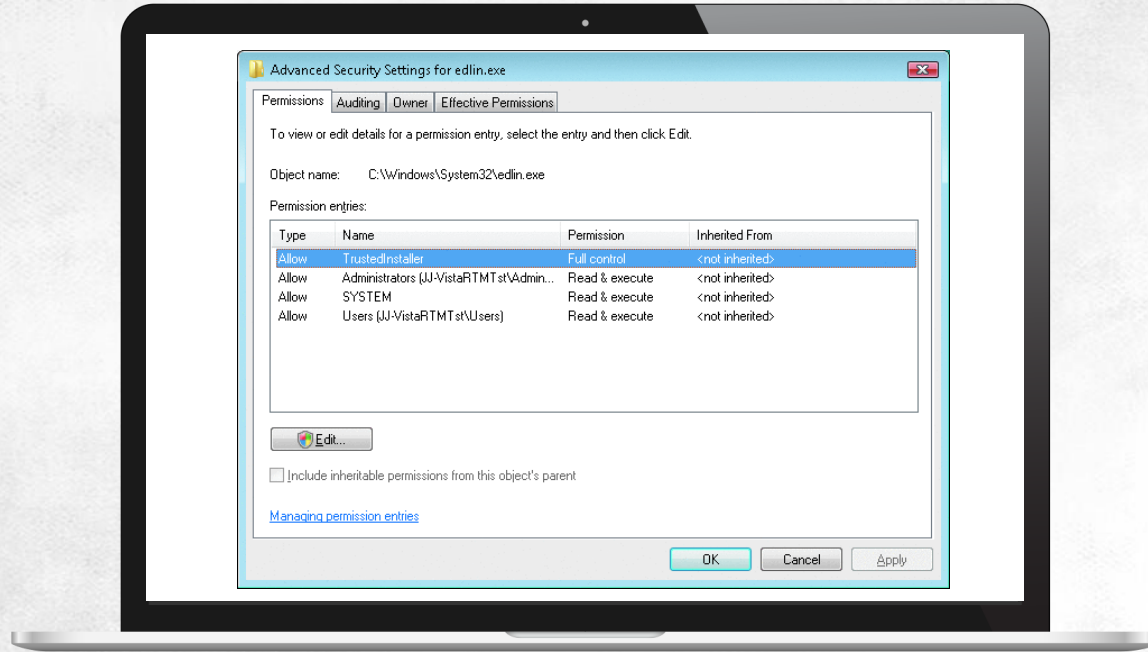
SYSTEM ADMINISTRATORS should force users to only be able to run trusted software by setting appropriate Software Restriction Policies

IF A MALICIOUS PROGRAM has already been started, you can reduce the damage it will produce if you make it run without elevated permissions



IMMUTABLE LAWS OF SECURITY

Law #2: If a bad guy can alter the operating system on your computer, it's not your computer anymore



IMMUTABLE LAWS OF SECURITY

Law #2: If a bad guy can alter the operating system on your computer, it's not your computer anymore

A computer is controlled by its operating system – this means for example that many system processes have full permissions to do anything in the system. Because the OS, like all other programs, is stored on the computer as files, altering these files will cause a change in how the entire system operates

Even though the current operating systems are protected from unauthorised modifications by some built-in mechanisms, none of them are fully effective. The most critical system files are protected using WFP. These files are signed digitally and WFP disables file modifications (except for system security fixes). WFP protects system files in two ways:



THE FIRST MECHANISM IS RUNNING IN THE BACKGROUND.

This protection is called if WFP receives a notification about any changes to the folder for a file in a protected folder



THE SECOND WFP PROTECTION MECHANISM

is a tool called System File Checker



IMMUTABLE LAWS OF SECURITY

Law #3: If a bad guy has unrestricted physical access to your computer, it's not your computer anymore



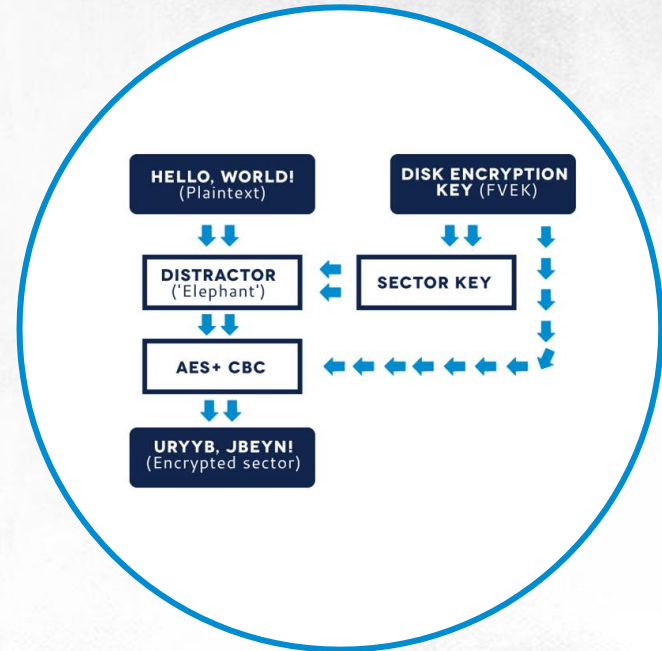
IMMUTABLE LAWS OF SECURITY

Law #3: If a bad guy has unrestricted physical access to your computer, it's not your computer anymore

THE ONLY EFFECTIVE COUNTERMEASURE IS ENCRYPTING THE SYSTEM DISK

This is made possible by the layered structure of the input/output subsystems of computers and operating systems. You can:

-  **ENCRYPT/DECRYPT** full hard disks (between layers 1 and 2)
-  **ENCRYPT/DECRYPT** selected logical disks (between layers 2 and 3)
-  **ENCRYPT/DECRYPT** selected files or folders (between layers 3 and 4)



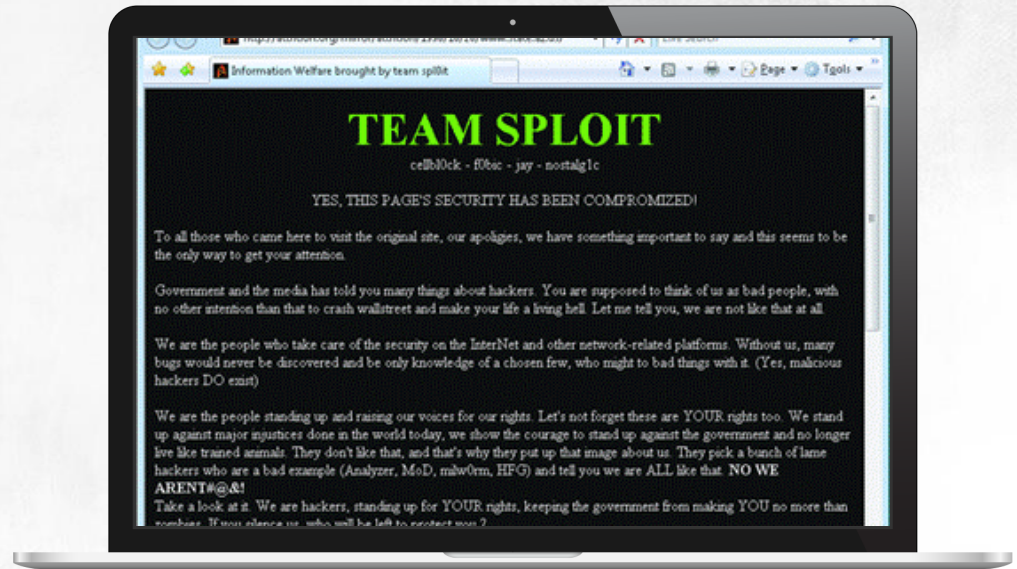
IMMUTABLE LAWS OF SECURITY

Law #4: If you allow a bad guy to run active content on your website or online application, it's not your website any more

IF YOU ALLOW an attacker to put up active elements on your website, it will become a malware-spreading vehicle attacking your visitors




HOWEVER, this step does not have to mean the attacker gains immediate control over your web server

IT ALSO DOESN'T MEAN the attacker will control the visitors' computers, or at least this will not happen unless they run a malicious program



IMMUTABLE LAWS OF SECURITY

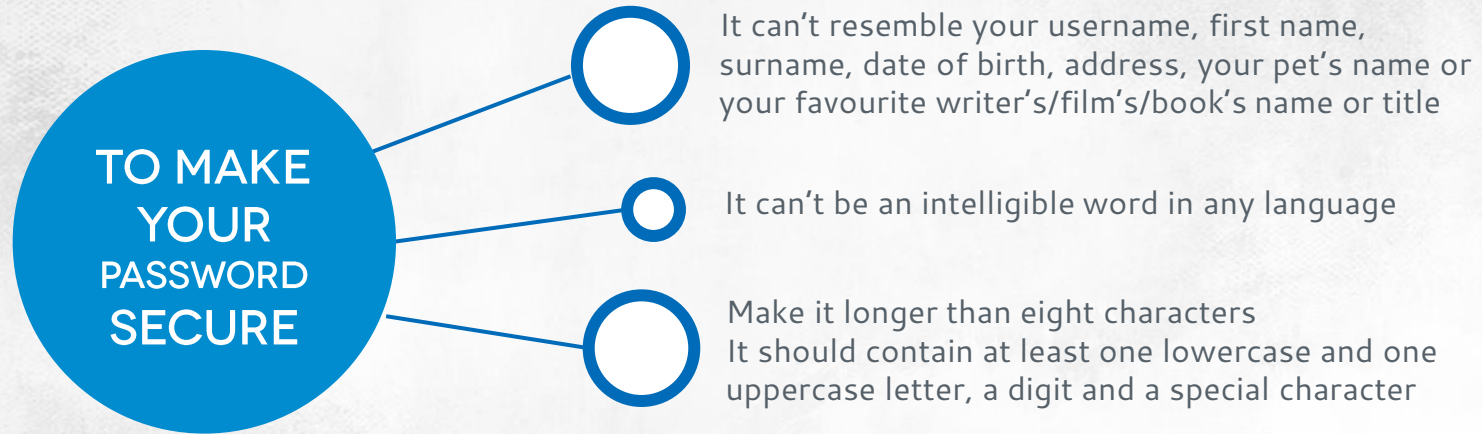
Law #5: Weak passwords trump strong security

-  **IN MOST CASES THE PASSWORD** is an operating system's only way of ensuring a user is who he claims to be. It follows that if someone else ever obtains your password, that person will be able to impersonate you in the system and gain access to all of your data
-  **A STRONG, SECURE PASSWORD** is a password only you know, and something others won't guess
-  **TO CRACK THIS PASSWORD,** the attacker will use the knowledge gained about you, dictionaries and programs that try many combinations of characters



IMMUTABLE LAWS OF SECURITY

Law #5: Weak passwords trump strong security



ADMINS SHOULD ENFORCE STRONG PASSWORDS THROUGH GROUP POLICY

That being said, cracking passwords is not the most serious problem you face. The problem are weak authentication mechanisms that limit the effectiveness of even the best security solutions

IMMUTABLE LAWS OF SECURITY

Law #6: A computer is only as secure as the administrator is trustworthy



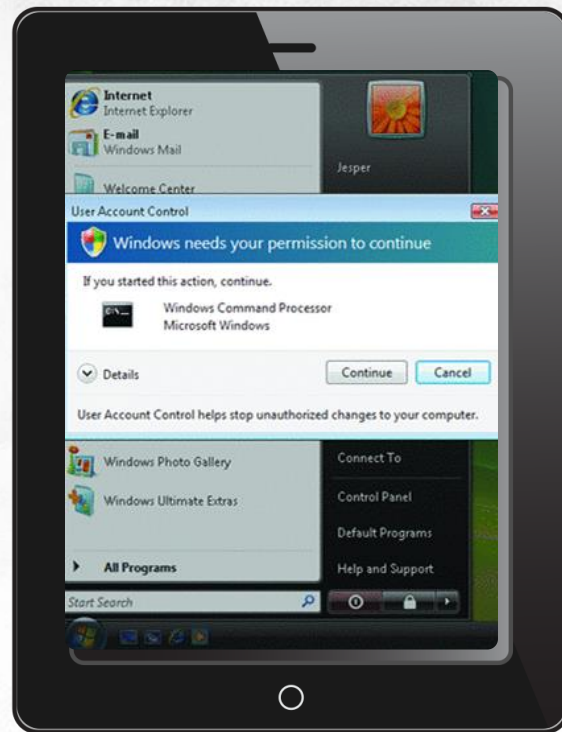
AN ADMINISTRATOR HAS FULL, unchecked control over a system, including the ability to remove traces of performed operations and logged events



EXPLOITS THAT NEED admin permissions to run are pointless



BUT WHEN AN ADMIN RUNS programs, the programs start with admin permissions... solutions like User Account Control may change this situation in the future



IMMUTABLE LAWS OF SECURITY

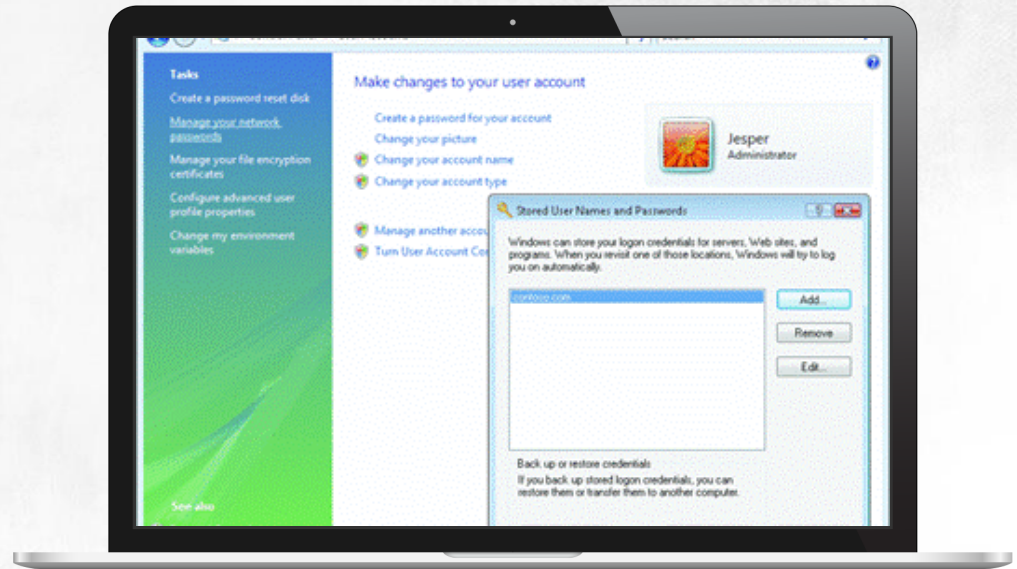
Law #7: Encrypted data is only as secure as its decryption key

AN OBVIOUS BUT FREQUENTLY OVERLOOKED PRINCIPLE

Many people store encrypted data and the keys that can be used to decrypt it on the same disk

While undoubtedly handy, this solution means that regardless of the used encryption algorithms, any attacker will be able to decrypt the data

A much better solution is to store keys in TPM modules, smart cards or even USB drives, provided the latter are not in the immediate vicinity of the encrypted computer



IMMUTABLE LAWS OF SECURITY

Law #8: An out-of-date malware scanner is only marginally better than no malware scanner at all



YOUR COMPUTERS NEED

to be constantly protected by an antivirus and anti-spyware software



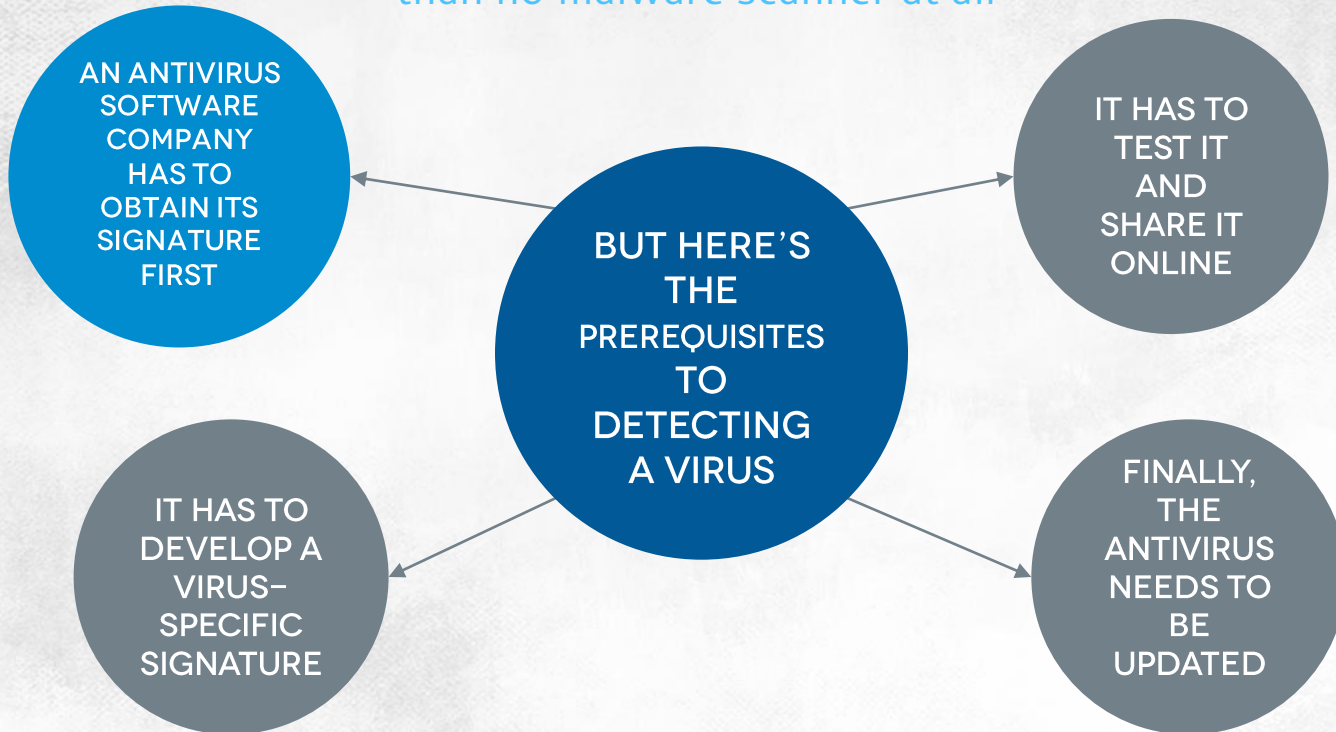
THE BASIC FUNCTION

of these programs is to compare all downloaded and opened files against a virus signature database that contains the characteristics of malware



IMMUTABLE LAWS OF SECURITY

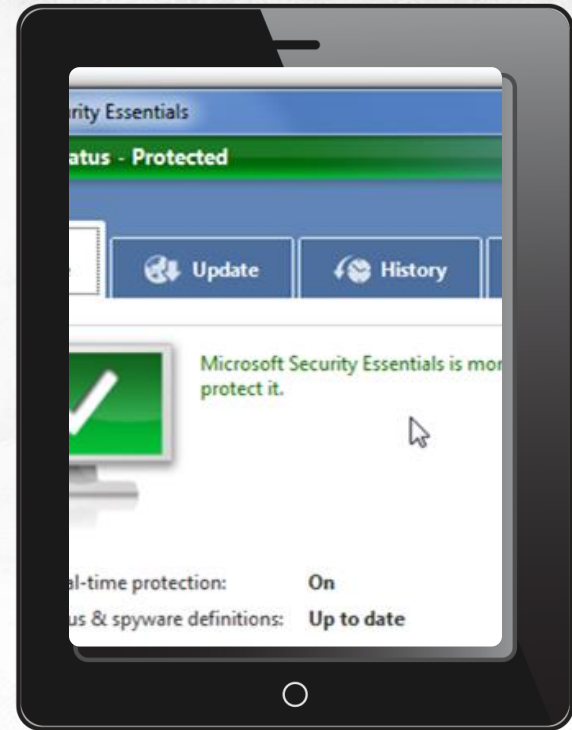
Law #8: An out-of-date malware scanner is only marginally better than no malware scanner at all



IMMUTABLE LAWS OF SECURITY

Law #8: An out-of-date malware scanner is only marginally better than no malware scanner at all

- ✓ SEVERAL DAYS OR EVEN WEEKS may pass from the time a malicious program is first launched until antiviruses are able to detect it
- 🚩 TO MAKE MATTERS WORSE, an increasingly bigger number of malicious programs are hiding by recompiling their entire codes regularly



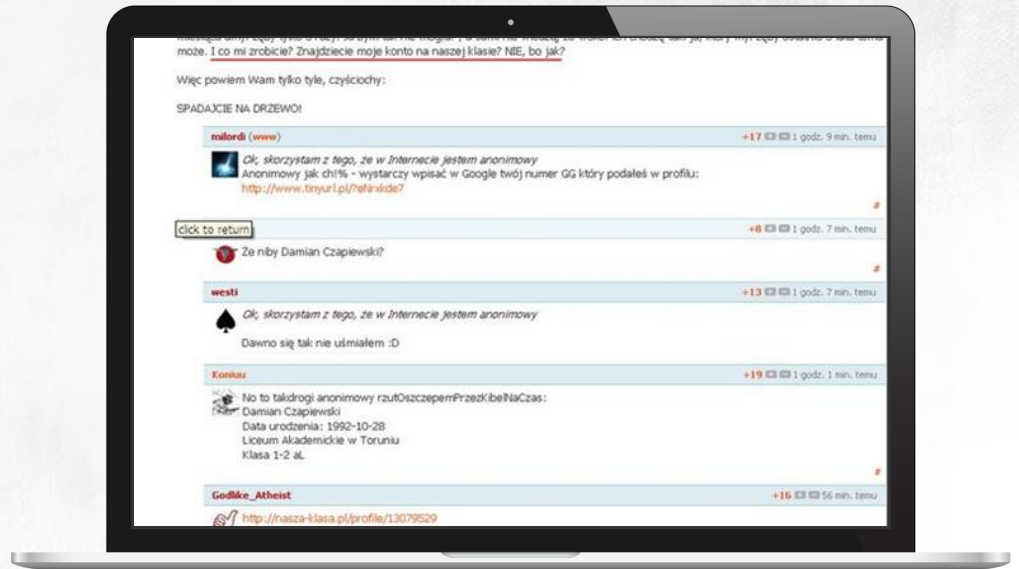
IMMUTABLE LAWS OF SECURITY

Law #9: Absolute anonymity isn't practically achievable, online or offline

PUBLISHING AND SHARING info with another person, it may be hard to retain your anonymity. This is also applicable online

HOWEVER, IF YOU EMPLOY certain tactics, like using a proxy server or onion routing, you can try and maintain anonymous

ONION ROUTING IS A NETWORK of virtual tunnels that enables you to use all services based on TCP/IP anonymously

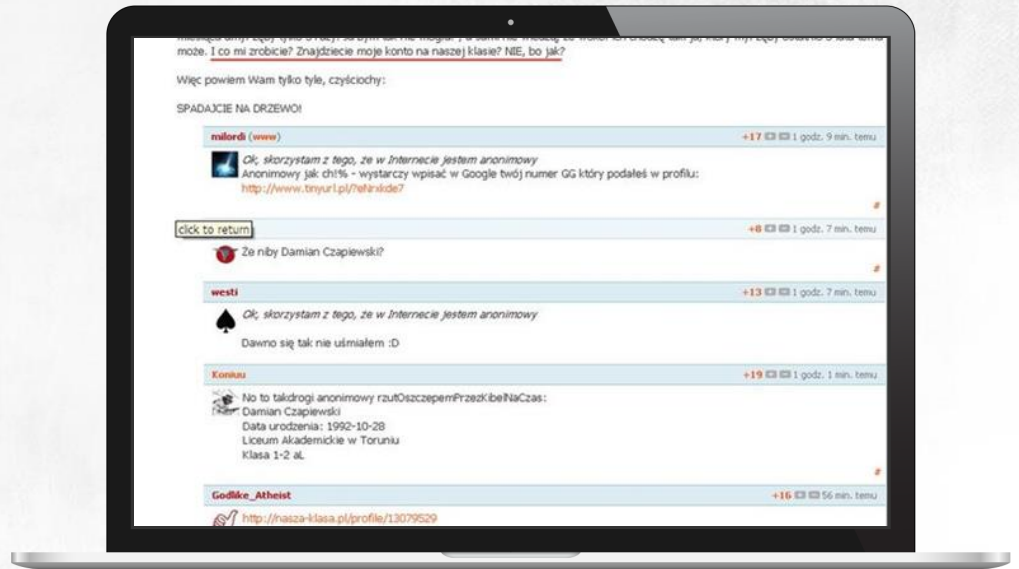


IMMUTABLE LAWS OF SECURITY

Law #9: Absolute anonymity isn't practically achievable, online or offline

A CLIENT PROGRAM DOWNLOADS

a current list of nodes from the network. It changes with other users turning on and off their servers. The client then maps a pseudorandom path through many servers, and once a packet is forwarded, the servers remove all traces of accepting it. To make it impossible to trace packets by adding a false server to the network, computers build the network of connections gradually. Each of them only knows the last server from which it received data



IMMUTABLE LAWS OF SECURITY

Law #10: Technology is not a panacea

While technology is the answer to an ever-growing list of problems and hurdles, it will not give you absolute security:



PERFECT SOFTWARE

and infallible computers is just a futuristic dream



SECURITY

is not a product, it's a process



IMMUTABLE LAWS OF SECURITY

Administration



SECURITY

isn't about risk avoidance; it's about risk management



SECURITY

only works if the secure way also happens to be the easy way



IF YOU

don't keep up with security fixes, your network won't be yours for long



NOBODY

believes anything bad can happen to them, until it does



IT DOESN'T

do much good to install security fixes on a computer that was never secured to begin with



THERE REALLY

is someone out there trying to guess your passwords



ETERNAL

vigilance is the price of security



THE MOST

secure network is a well-administered one



THE DIFFICULTY

of defending a network is directly proportional to its complexity



TECHNOLOGY

is not a panacea



THANKS

