

The Little Illustrated Guide



IT Security

How to be prepared for
cyber attacks



IT SECURITY

IT security concerns you. In fact, like it or not, it concerns everybody, however sceptical they may be.

Theft of hardware or data, virtual identity theft, and even surveillance of online activity, are no longer crimes to which only celebrities fall victim, but ones which may be perpetrated against any one of us.

As key players at a reputable Swiss école polytechnique, we all have a duty to be aware of the risks in terms of internet security, and to know how to react when faced with the increasing number of threats, virtual or otherwise, to which we are exposed. This guide offers some simple advice and concrete examples to help you minimise the risks associated with using computers.

Summary

- 1 Passwords**
- 2 Your Workstation**
- 3 Remote Use: USB sticks and external hard drives**
- 4 Connecting to a public Wi-Fi network**
- 5 Copyright and Downloading**
Keeping an eye on your Inbox!
- 6 Malicious e-mails**
- 7 Phishing**
- 8 Hoax**
- 9 SPAM**
- 10 The jungle that is the web**
- 10 Cookies**
- 11 Using the internet without fear or blame**
- 11 Protected sites and encrypted connections**
- 12 Classifying data for self-protection**
- 13 Glossary**

Impressum :

Authors: Magaly Mathys, Céline Deleyrolle, Julien Robyr (IT Communication, VPSI)

Illustrations: Igor Paratte (Pigr)

Graphics: Julien Robyr

Printing: Print Center, EPFL

In collaboration with Patrick Saladino and Jean-François Dousson (IT Security, VPSI)



PASSWORDS

WHY IS IT IMPORTANT?

Your password is like the key to a safe: personal, non-transferable, there is only one per model and its related code must be unique, secret and sufficiently complex.

It really is your most efficient weapon against a cyber attack. Choose it carefully!

And use more than one!

HOW TO CHOOSE A PASSWORD

Avoid using the same password for everything, even though a single password is easier to remember. And above all, change your passwords regularly (at least once a year).

Avoid short words, obvious words, first names and dates of birth. Don't make it easy for the hackers!

What makes a good password?: It must contain a minimum of a dozen characters – a combination of upper and lower case letters, numbers and special characters. Avoid sequences of numbers or letters, and don't use words from the dictionary or proper names.

BONUS TIP

Create phrases and sentences, for example:

lw0rk@3PFL! (= "I work at EPFL!").

Here is a list of the worst most frequently used passwords:

12345678	BATMAN
PASSWORD	111111
QWERTZ	ACCESS
FOOTBALL	696969
ABC123	MOTDEPASSE
LETMEIN	12345

(source: splashdata)



YOUR WORKSTATION

SOME WORK HABITS

THAT WILL GREATLY REDUCE THE RISK OF HACKING

- Secure the screen and the central processing unit with a security cable. Keep the key in a safe place.
- Only use your administrator account when you really need to, and log out afterwards.
- Activate the password-protected screensaver after no more than 45 minutes.
- Never install pirated software or software whose source you are unsure of.
- In Windows, install EPFL's official antivirus software.
- Activate automatic updates.

A new management post has just become vacant at EPFL. Two employees have applied for it: Robert and Aline. They are acquainted, but don't have very high opinions of each other because of old professional disagreements.

One evening, after working late, Robert passes Aline's office and notices that her desktop PC is still on. It only takes him a few minutes to find some embarrassing personal information and send it to management using Aline's user-name. A week later, Aline resigns and Robert gets the job.



THE RISKS

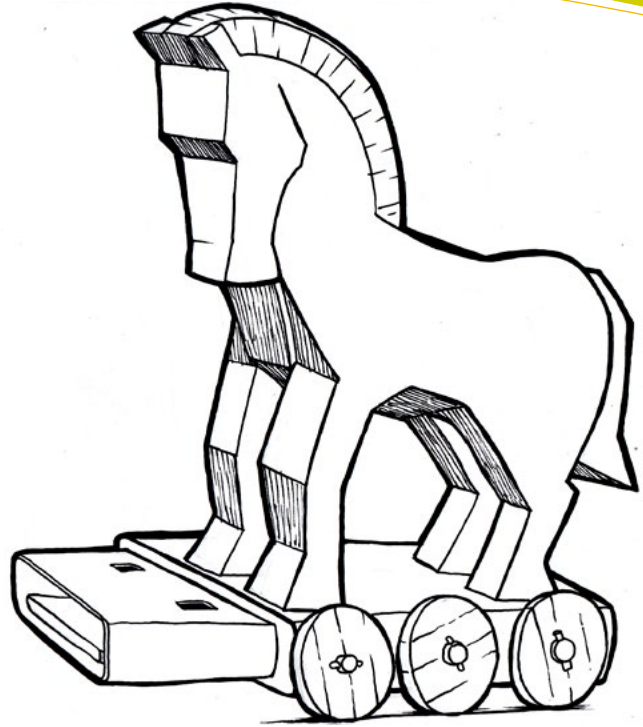
It can take less than a minute for an unattended workstation to become the target of someone who's up to no good. Cases of hardware theft are the most common because hardware is the most visible, but theft of data and unauthorised access to EPFL's web services represent serious risks for both users and EPFL.

USB STICK EXTERNAL HARD DRIVE REMOTE USE



Even if a file isn't opened, a USB stick can contain an autorun, and malware programmed to steal sensitive documents and identifiers (usernames, etc.). Also, a hidden port can be installed on the laboratory's server.

Corinne is a PhD student in nuclear physics. During a coffee break she finds a USB stick on a table. With perfectly laudable intentions, she plugs it into her laptop to see who it belongs to. What she hasn't realised is that the stick contains spyware.



SO WHAT SHOULD YOU DO?

- **In your operating system, de-activate the autorun for any content stored on peripherals.**
- **As far as possible, never store sensitive information on a USB stick.**
- **Make sure all content is erased from the stick before lending it. Formatting is strongly recommended.**
- **Always shut down your workstation before leaving it, to prevent a USB stick being inserted into it during your absence.**



LAPTOPS, TABLETS & MOBILE PHONES PUBLIC WI-FI

THE RISKS

All communications that you establish via an unsecured network (public Wi-Fi or wired connection in a hotel) can be intercepted without your knowledge.

SOME ADVICE

- Use EPFL's VPN service to encrypt all your communications.
- Activate the encryption function on phones and tablets.
- De-activate file sharing.
- De-activate the wireless network when you're not using it.

WORTH KNOWING

Data is not only exchanged via e-mails and web browsing, but also via all technical data sent and received by a computer to enable it to function.

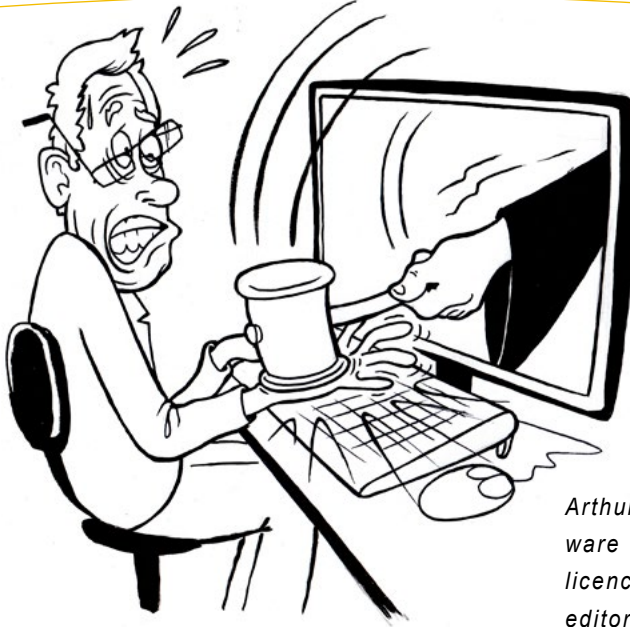


Alan is head of a bio-engineering laboratory. While on a work trip, he connects to the free Wi-Fi at the airport to check his e-mails using his tablet. Six months later, a foreign laboratory patents the system he'd been working on for three years.

WI-FI AT HOME

When installing your Wi-Fi at home, for extra security, always choose the WPA2/AES protocol. Then, on the router, don't allow the default administrator access (often "admin", with the password "admin") - and protect this account with a strong password of more than 12 characters.

COPYRIGHT & DOWNLOADING



Respect for intellectual property is one of the basic values that EPFL rates most highly. By recognising the rights of third parties, EPFL helps protect what it produces via its contributors – that is; its researchers, its students and its employees.

Arthur, a PhD student in a laboratory, decides to use some software called Easydrag&Drop for his research. He finds a pirated licence on the internet and installs it on his workstation. The editor spots the illegal version and decides to block all EPFL's licences for as long as Arthur hasn't paid for the pirated version.

DEFINITION

A lot of people think that copying software, a film or a musical work is an innocent act without consequences. That is absolutely not the case. Any act of piracy involves the full personal responsibility of the perpetrator, who may then face prosecution.

WHAT YOU ARE RISKING

In the event that EPFL's infrastructure is used for acts of piracy, the perpetrators are not only breaking Swiss and/or foreign laws, but also internal directives, as well as damaging EPFL's image and undermining the property rights of third parties. We remind you that the EPFL does not tolerate any act of this sort, and has the right to prosecute perpetrators.

PLEASE NOTE

This applies to all of the following: films, images, photos, icons, music, software, operating systems, digital books and all content protected by copyright.



KEEPING AN EYE ON MY INBOX

MALICIOUS E-MAILS

What we have here is an electronic message, the contents of which (either an attachment or a link within the body of the message) was designed for the purpose of tricking the recipient and taking advantage of the resources of their information system. In this instance, we are primarily thinking of Trojan horses, which are designed to make use of the computer's resources (network connection and stored data) for dishonest ends, but also phishing sites, set up for the purpose of stealing users' personal identifiers through one of the pages they host.



Over a period of several months, hackers gathered information on one or more employees of TV5 Monde. They simply used Google, the various social networks and other "traditional" ways, such as targeting Skype accounts to find out more about their target.

They then sent their targets a very authentic-looking e-mail inviting them to download an attached file that was, in fact, a Trojan horse. Once workstations such as the community manager's were infected, the hackers were able to install keyloggers and malware. In this way they were able to obtain the usernames and passwords they needed to take control of TV5 Monde's social networks.

1. Strange message title given the sender

2. Attachment with a strange name

3. Vague, odd, unexpected message from a so-called colleague. No sign-off phrase or signature.

PHISHING

KEEPING AN EYE
ON YOUR INBOX



THE RISKS

Hackers can use your Inbox, steal your identity and get access to all your data. They can sell this information or use it to get into EPFL's IT system and infect it with a virus. The huge diversity of such attacks makes it difficult to put a figure on the resulting financial impact.

THE DISTINCTIVE SIGNS

THE URGENCY OF THE ACTION TO BE TAKEN

and/or the risk you'll lose data or e-mails if you don't act quickly.

SIGNATURE IN THE EMAIL IS GENERIC AND IMPERSONAL

All official communications from VPSI are signed by one of its employees, who can be reached by telephone to verify the legitimacy of the message.

OFFICIAL COMMUNICATIONS ARE BILINGUAL

Wherever possible, all official e-mails are written in the two languages used at the EPFL (French and English).

FREQUENT SPELLING MISTAKES

and/or bad grammar and sentence construction of the Google Translate type.

A LINK OUTSIDE EPFL

Finally, if you are asked to send your personal identifiers via a website, you will note that this website is not hosted by the EPFL (the address of the site doesn't end in .epfl.ch)

SO WHAT SHOULD I DO?

Immediately erase e-mails of this sort and, above all, don't open either attachments or links inserted into the body of the email.

If in doubt, contact the VPSI Service Desk on 1234 or 1234@epfl.ch

Upgrade Email Account Now

System Administrator <systemadmin@epfl.ch>

Envoyé : [redacted]
À :

Dear User,

1. Urgent action required

Your mailbox has exceeded the storage limit which is 20GB as set by your administrator, you are currently running on 20.9GB, you may not be able to send or receive new mail until you re-validate your mailbox.

To re-validate your mailbox please CLICK HERE:

<http://u2010.eb2a.com/feedback/feedback.html>

2. Web site external to EPFL

Thanks

System Administrator

3. Impersonal signature

Matthieu is studying at EPFL. In addition to studying, he has several little jobs, one of which is in one of the cafeterias at EPFL. One morning, he receives an e-mail from one of EPFL's restaurants telling him it forgot to pay him the sum of CHF 117. All he has to do is to click on a link and log in for the transfer to be made. The page to which he is redirected looks very much like EPFL's login page. He logs in, and his personal data is copied by the hacker.



HOAX

KEEPING AN EYE ON YOUR INBOX

A hoax is an e-mail essentially spreading false and often unverifiable information. It may contain alerts to non-existent viruses, a support network or an exceptional (and false) offer. A hoax does not, by definition, represent a danger to your computer, your finances or your future.

The risks associated with internet hoaxes lie elsewhere, but are nonetheless real.

THE RISKS

DISINFORMATION

People want to believe it and thus spread it and the attention that goes with it.

UNNECESSARY FILLING OF INBOXES

CLOGGING OF THE NETWORK

In the same way as spam – with unnecessary traffic.

DAMAGE TO ONE'S IMAGE

What would you think if you were the subject of the hoax?

FALSE ALARMS

And by crying wolf...

HARM CAUSED TO NET SURFERS

Pretending that a system file contains a virus and advising net surfers to delete it.

De [REDACTED]

Répondre

Transférer

Archiver

Indésirable

Supprimer

Sujet **IMPORTANT MESSAGE TO SPREAD**

17:17

Pour [REDACTED]

Autres actions ▾

Message to pass on!!!

In the next few days you should be very careful not to open any message with the subject: "The invitation" or "What's your photo doing on this site?" It doesn't matter who it comes from!!! It's a virus that opens an Olympic torch and burns the hard disk of the PC. This virus will be sent by someone on your list of contacts, and that is why you absolutely must send this email. It's better to receive this message 25 times than to receive the virus and open it!!!

So if you receive a message with the subject "Invitation" UNDER NO CIRCUMSTANCES OPEN IT AND SWITCH OFF YOUR PC IMMEDIATELY. It is the worst virus reported by CNN and classified by Microsoft as the most destructive virus that has ever existed!

This virus was discovered yesterday afternoon by McAfee and as yet no solution has been found that will alleviate its effects. It quite simply destroys the 'zero zone' on the hard disk, where the vital data is stored ! SEND THIS EMAIL TO EVERYONE YOU KNOW!!!! To your friends, your contacts. . . Because the more people you warn, the more the virus will have difficulty spreading. Cut and paste this text into a new message before sending it.

WHERE TO FIND OUT MORE ?

1234@epfl.ch

Hoaxbuster

www.hoaxbuster.com

HoaxKiller

www.hoaxkiller.fr

KEEPING AN EYE ON YOUR INBOX SPAM




Although they are very widespread, and have attracted lots of media attention, spam e-mails are becoming ever more powerful. Their aim is quite simply to sell things to you – anything from medicines, diplomas and loans to computer software, and tips on how to get money for nothing.

Once your e-mail address is out there on the net, it's no longer possible to prevent its being used. Nevertheless, here are a few pieces of advice to help you minimise the risks associated with spam e-mails.



THIS HEAVY-WEIGHT NETWORK COLOR PRINTER CAN TAKE ON ANYONE, ANYTIME, FOR ONLY \$599*.



You can create knock-out brochures and presentations, in crisp, vibrant color.

It's a natural.

Learn about the
**Phaser® 8500
Network Color Printer**

PERFORMANCE:

- Up to 24 PPM color
- 600 MHZ processor

PRODUCTIVITY:

- Network standard
- 85,000 page duty cycle
- 625 sheet paper capacity

TECHNOLOGY:

- Solid Ink printing

WARRANTY:

- One-year onsite
- Total satisfaction guarantee

ONLY \$599*
after \$300 rebate*

NEVER BUY WHAT IS OFFERED FOR SALE

It only takes a tiny percentage of people to respond for it to be worthwhile for the spammers. If nobody responds it will make it less profitable for them and they will be less motivated to send spam.

NEVER ATTEMPT TO UNSUBSCRIBE

Most of the time this will only confirm to the spammers that your email address is valid, and that there is indeed a human being behind it reading their emails. For them, this immediately adds value to your email address.

NEVER LEAVE YOUR EMAIL ADDRESS ON FORUMS

Robots exist that are programmed to do the rounds of websites collecting email addresses for spammers.

UPDATE YOUR EMAIL SOFTWARE

Any software that isn't up to date represents an opportunity for spammers, even the least experienced. Don't play with fire!

If you have a website or a blog, DON'T LEAVE YOUR EMAIL ADDRESS ON IT

...in text form. Only put it on there in the form of a picture. This will prevent robots scanning the web from finding it.

NEVER PASS ON A HOAX

...by responding to an invitation to pass on an e-mail to as many contacts as possible. Such lists of contacts are basically just gifts to collectors of addresses.

CREATE ONE OR MORE «DISPOSABLE ADDRESSES»

to be used only for signing up or logging in to sites you feel you can't trust.



COOKIES THE JUNGLE THAT IS THE WEB

USING THE INTERNET WITHOUT FEAR OR BLAME

COOKIES

Like little crumbs, cookies are small files placed in your browser by certain sites to analyse where you go when browsing.



RISKS & IMPACT

They can be useful (e.g. recording the URLs of sites already visited), but this usefulness is disputable, as cookies allow your trail to be followed and your profile established.



SO WHAT SHOULD YOU DO?

Don't forget to regularly delete these cookies (an option on your browser).



USING THE INTERNET WITHOUT FEAR OR BLAME

Here are a few security tips for browsing without getting your data crunched :

Keep your operating system up to date, together with all web applications. In other words, do the updates when the system tells you to.



Use safe passwords – and a different one for each website.



Take heed of any warnings from your browser.



Beware of doubtful-looking sources of downloads. Install the EPFL's official antivirus software and don't de-activate it.



THE JUNGLE THAT IS THE WEB

PROTECTED SITES
ENCRYPTED CONNECTION
IDENTITY THEFT

1 1 0 1
0 0 1 1
1 0 0 1
1 1 1 0 1 0 0



PROTECTED SITES ENCRYPTED CONNECTION

Check the certificates of the servers. Digital certificates are generally used when an encrypted connection (https) is set up, so the server can prove its identity to the clients of its services (online payment, consultation of certain data, etc.) and thus its legitimacy.



SO WHAT SHOULD YOU DO?

Refuse to communicate any sensitive data to a site presenting an incorrect certificate (you will receive a message to this effect from your browser), as it could well be a phishing site.



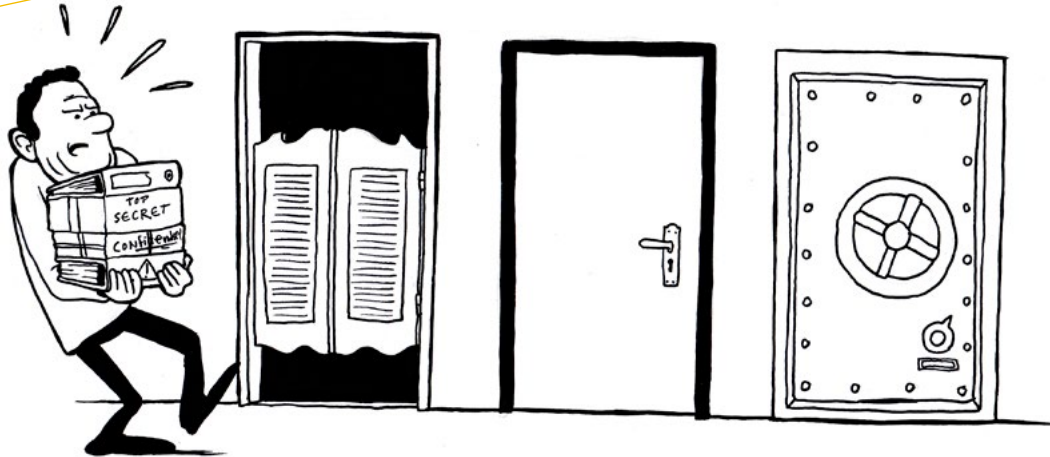
IDENTITY THEFT

Bear in mind that identity theft is common. It can happen that your identity is stolen and used with ill intentions, to send SPAM, as a joke or to cause harm.



CLASSIFY INFORMATION

FOR SELF-PROTECTION



René is a computer science student. He regularly helps Xavier, a student friend of his who is doing a PhD in architecture, with IT queries.

One evening, René is alone on Xavier's computer. Out of curiosity, he looks at the last documents to be opened. They are not protected, and mention a new building project on the campus. Very interested, he sends them all to a journalist friend who wastes no time in publishing the information.

Classification of information is a process that allows information to be distributed according to a series of levels, each characterising a desired level of protection. It makes it possible to prioritise the protection of information of particular value.

RISKS

Incorrect classification of information makes the work of attackers easier. They see in it a tempting gateway to all types of sensitive and unsecured information, such as an employee's state of health, a teacher's evaluation slip, a police record or bank details.

ADVICE

- Always classify information according to its value.
- Adapt the security measures you take with your information to its classification in each case.
- Re-classify information over time if its value changes.



GLOSSARY

Cookies

Cookies are small files placed in your browser by certain websites, either to save having to reconnect to each page or to analyse your movements online.

Hoaxes

Hoaxes are false statements appealing to feelings of insecurity or compassion on the part of the recipient, with the aim of encouraging them to pass on the message to all their contacts.

Malware

Malicious programme introduced into a computer without the user's knowledge. This category includes viruses, worms, Trojan horses, CryptoLocker, ransomware, backdoors, etc.

Phishing

Phishing is a scam in which the sender passes themselves off as a trustworthy person (e.g. a personal contact, a bank or an @epfl.ch service) in order to obtain confidential data.

SPAM

SPAM messages are unsolicited messages with the aim of tricking the user into clicking on a link to an advertisement or of overloading IT infrastructures.



HELP !!

**If you have a query or problem
of any kind, please don't hes-
itate to contact the VPSI
Service Desk**

021 693 1234
1234@EPFL.CH

POLYLEX

As no-one should be ignorant of the law, we urge you to consult the EPFL's current Information Systems Security Policy (LEX 6.5.1), and its Directive On The Use of EPFL's Electronic Infrastructure (LEX 6.1.4) at <http://polylex.epfl.ch>.

SWISS LAW

The Swiss Civil Code (Art. 28) prohibits attacks on the personality of a third party.

The Swiss Penal Code prohibits attacks on a person's honour and defamation (Art. 173), slander (Art. 174), insult (Art. 177) and discrimination (Art. 261a).

The Swiss Data Protection Act (LPD Art. 12) prohibits the use of the data of third parties for illicit purposes or even its use against their will (for example, stealing the profile of a third party and using it to impersonate them).

The Swiss Copyright Act (LDA, Art. 67) prohibits the dissemination, modification or provision of a work (for example, the unauthorised downloading of music, films, software, etc.).

The Swiss Federal Personnel Act (LPers, Art. 22) states that Confederation personnel are subject to professional secrecy, commercial secrecy and official secrecy.