Funded by
the European Union

# DigiSkiPasS – Digital Skills Passport for Senior

*2023-1-BE01-KA210-ADU-000153530*

*[www.digiskipass.com](http://www.digiskipass.com)*

Funded by
the European Union

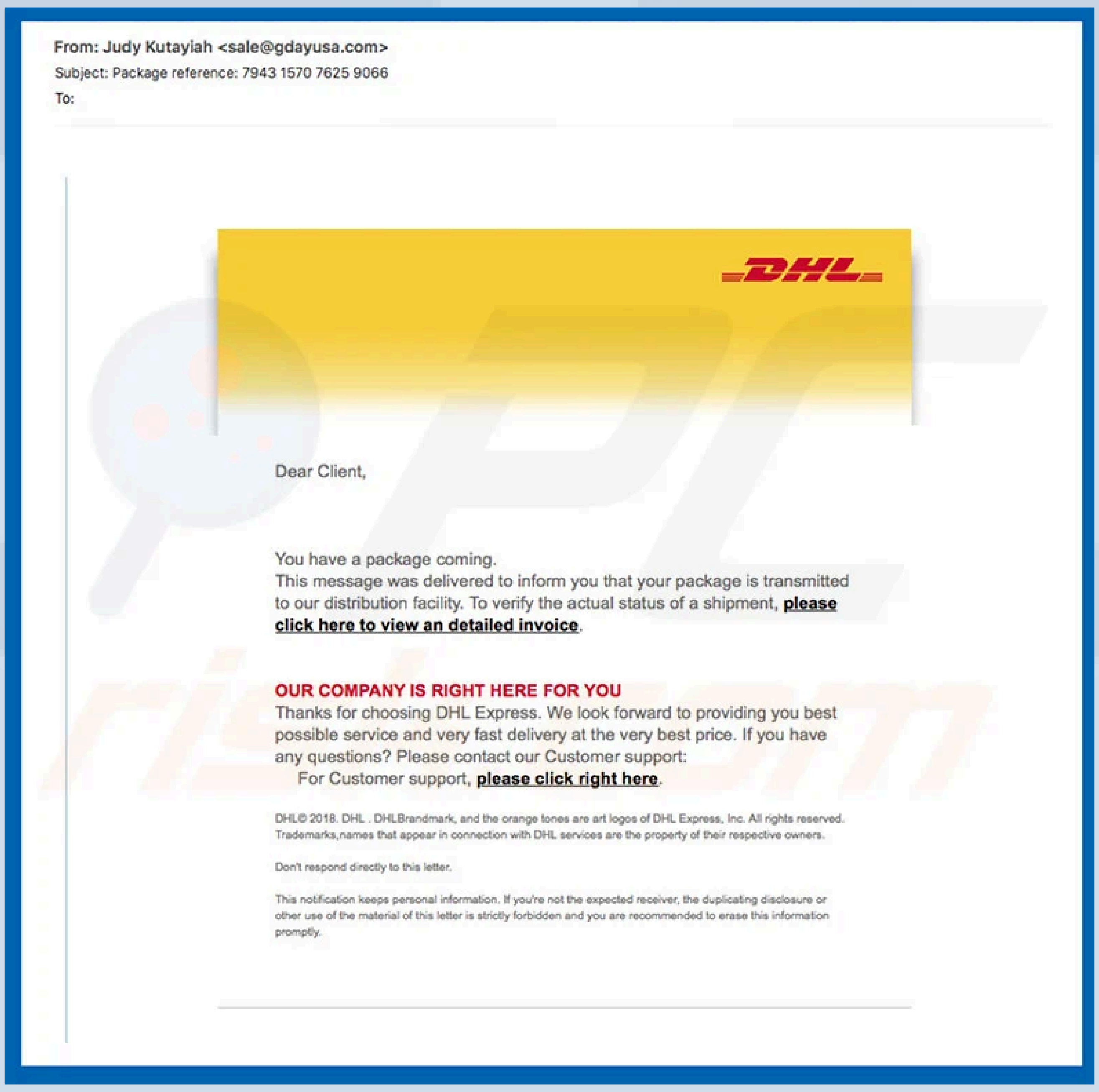
# KNOW AND APPLY CYBER SECURITY

Funded by
the European Union

# DEVICE SECURYTY

## MALWARE

Malware is the abbreviated form for "malicious software", and any other software capable of impairing the operation of computers or mobile devices, acquiring sensitive information, enabling access to private systems, or forcing the display of unwanted advertisements. Some of them are harmless, but others can cause substantial harm.



From: Judy Kutayiah <sale@gdayusa.com>
Subject: Package reference: 7943 1570 7625 9066
To:

Dear Client,

You have a package coming.
This message was delivered to inform you that your package is transmitted to our distribution facility. To verify the actual status of a shipment, **please click here to view an detailed invoice**.

**OUR COMPANY IS RIGHT HERE FOR YOU**
Thanks for choosing DHL Express. We look forward to providing you best possible service and very fast delivery at the very best price. If you have any questions? Please contact our Customer support:
For Customer support, **please click right here**.

DHL© 2018. DHL . DHLBrandmark, and the orange tones are art logos of DHL Express, Inc. All rights reserved. Trademarks,names that appear in connection with DHL services are the property of their respective owners.

Don't respond directly to this letter.

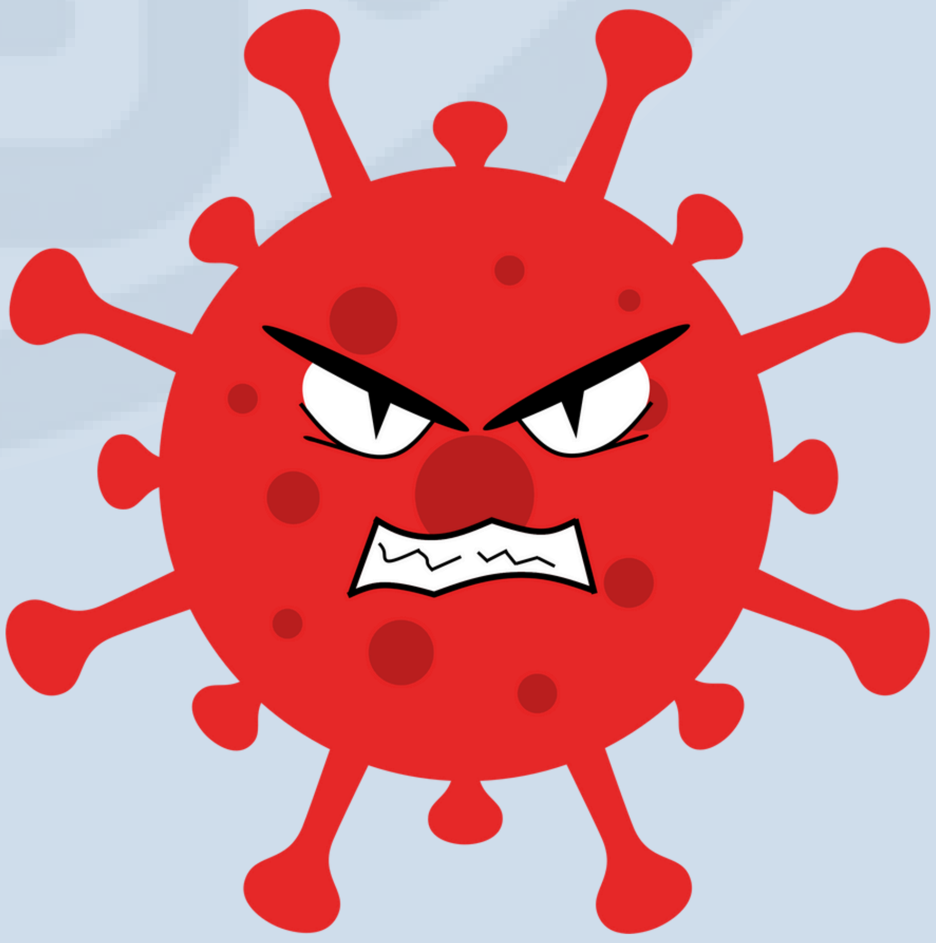
This notification keeps personal information. If you're not the expected receiver, the duplicating disclosure or other use of the material of this letter is strictly forbidden and you are recommended to erase this information promptly.

Funded by
the European Union

***Let's take a closer look at the most common malware.***

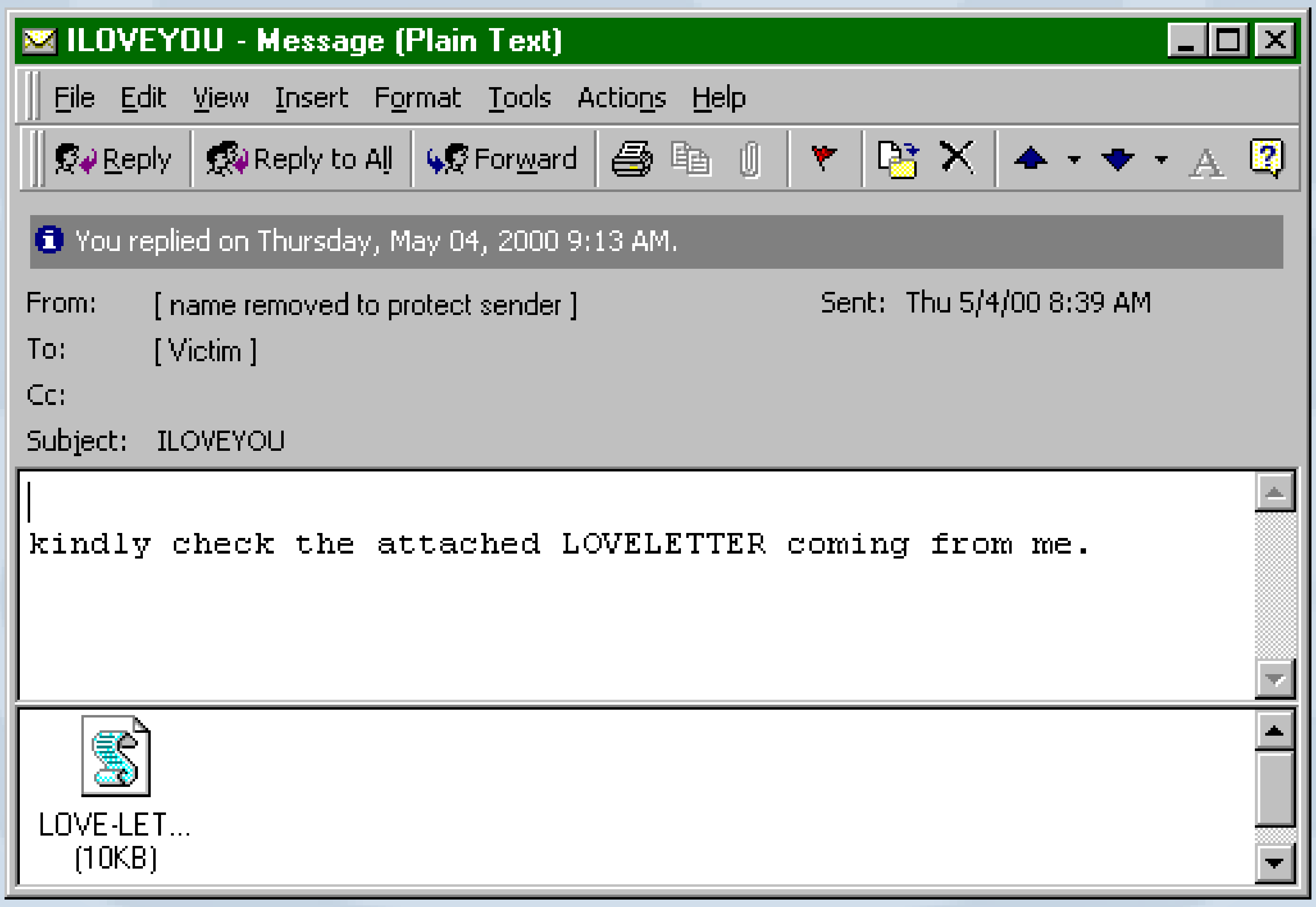
The **TROJAN** - like the Trojan Horse of Greek mythology, this type of malware stands out from others in that it is a program designed to trick users into installing it. The **TROJAN** can be used to steal personal information. This is achieved by creating a backdoor to your system that allows hackers to control it. Usually, computers get infected with Trojans through email attachments.

**VIRUS** - like the virus that can infect a person, the computer virus is also very contagious. It is a piece of code that infects the host software and then spreads the contagion through the system's files. If files are shared through one system, the virus can also be transmitted to other devices.



Funded by
the European Union

Viruses can be spread through email attachments, USB sticks, cloud storage, and others. It's a good idea to always verify the files you receive. For example, if you are sent a video, know that if the name includes "**.exe**", such as in the name "**.mov.exe**" it will almost certainly have something to do with a virus.


ILOVEYOU - Message (Plain Text)
File Edit View Insert Format Tools Actions Help
Reply
Reply to All
Forward

You replied on Thursday, May 04, 2000 9:13 AM.

From: [ name removed to protect sender ] Sent: Thu 5/4/00 8:39 AM
To: [ Victim ]
Cc:
Subject: ILOVEYOU

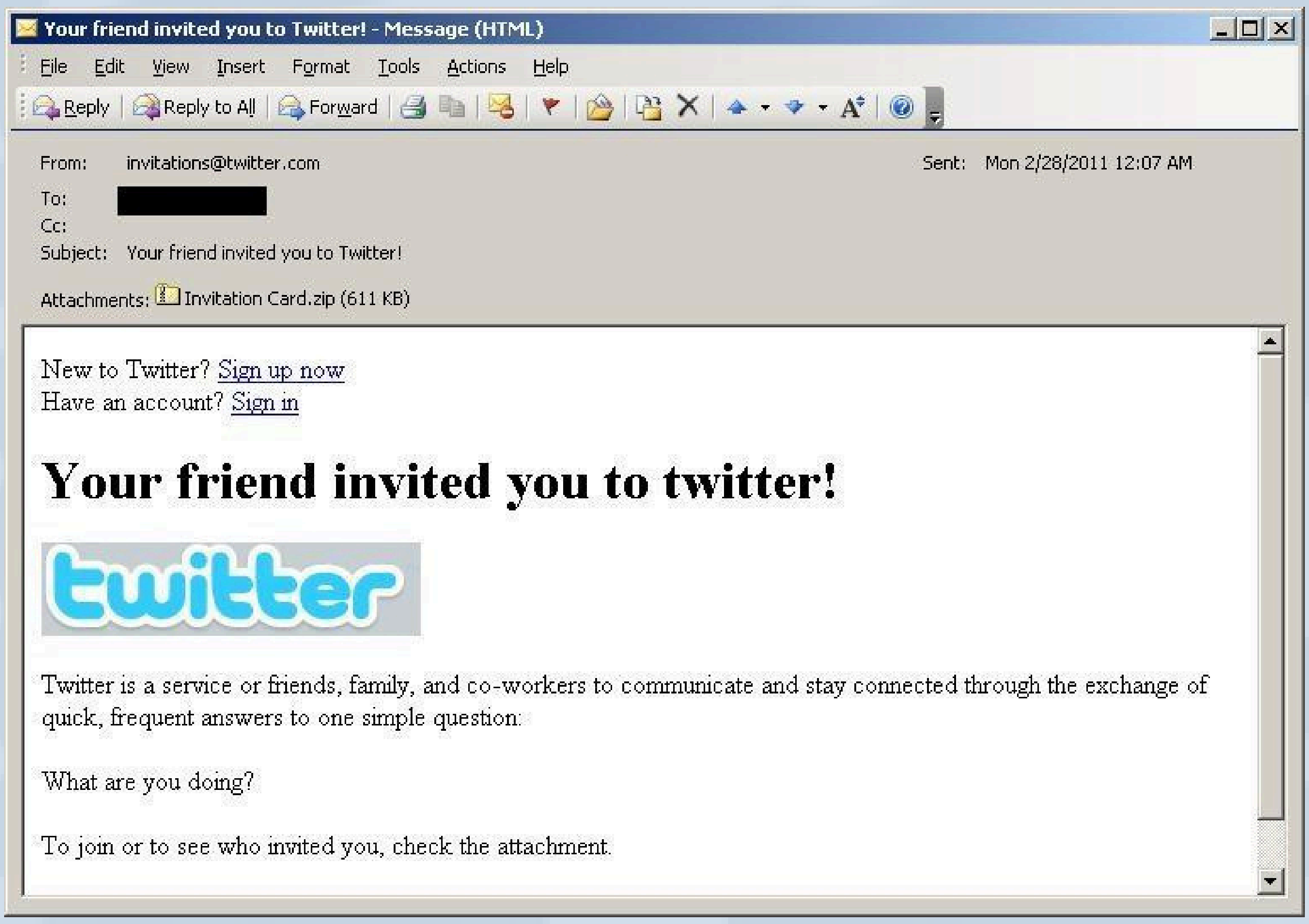
```
kindly check the attached LOVELETTER coming from me.
```

LOVE-LET...
(10KB)

For example, the ***ILOVEYOU virus*** was one of the first viruses to spread via email. The moment suspicious users click on the attachment, it spreads infecting the computer's audio, image, and all other files.

Funded by
the European Union

**WORM** is the most common type of malware. It causes damage similar to that caused by viruses. The difference lies in the fact that computer worms have the ability to self-repeat, self-multiply, and spread independently, whereas viruses rely on human activity to spread (e.g., run a program, open a file).


Your friend invited you to Twitter! - Message (HTML)
File Edit View Insert Format Tools Actions Help
Reply Reply to All Forward

From: invitations@twitter.com
Sent: Mon 2/28/2011 12:07 AM
To: [redacted]
Cc:
Subject: Your friend invited you to Twitter!
Attachments: Invitation Card.zip (611 KB)

New to Twitter? Sign up now
Have an account? Sign in

**Your friend invited you to twitter!**

twitter

Twitter is a service or friends, family, and co-workers to communicate and stay connected through the exchange of quick, frequent answers to one simple question:

What are you doing?

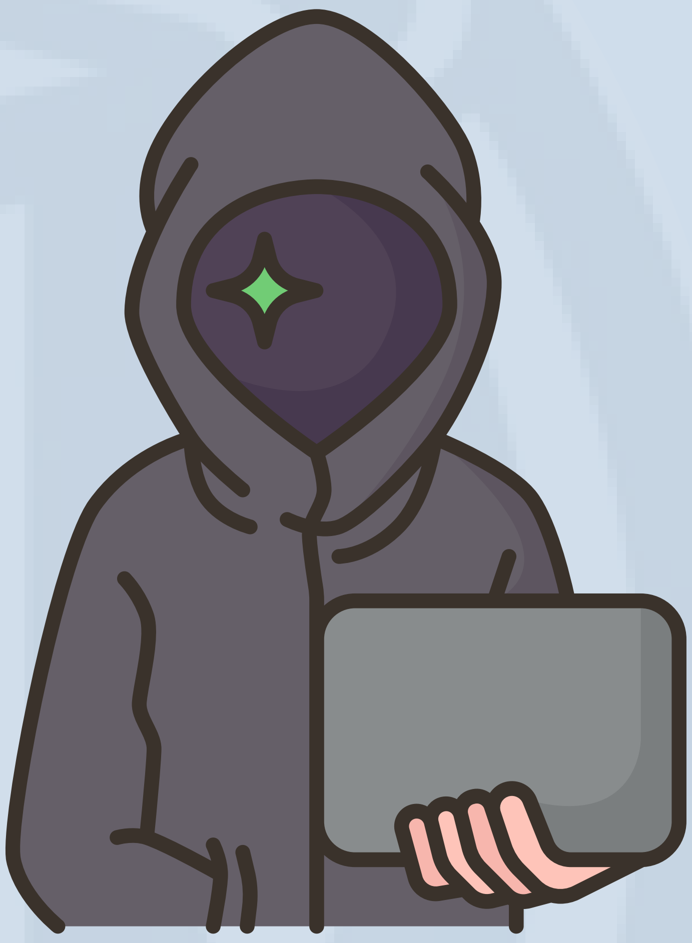
To join or to see who invited you, check the attachment.

Worms are most commonly spread by sending e-mails with infected attachments to users' contacts in the address book.

Funded by
the European Union

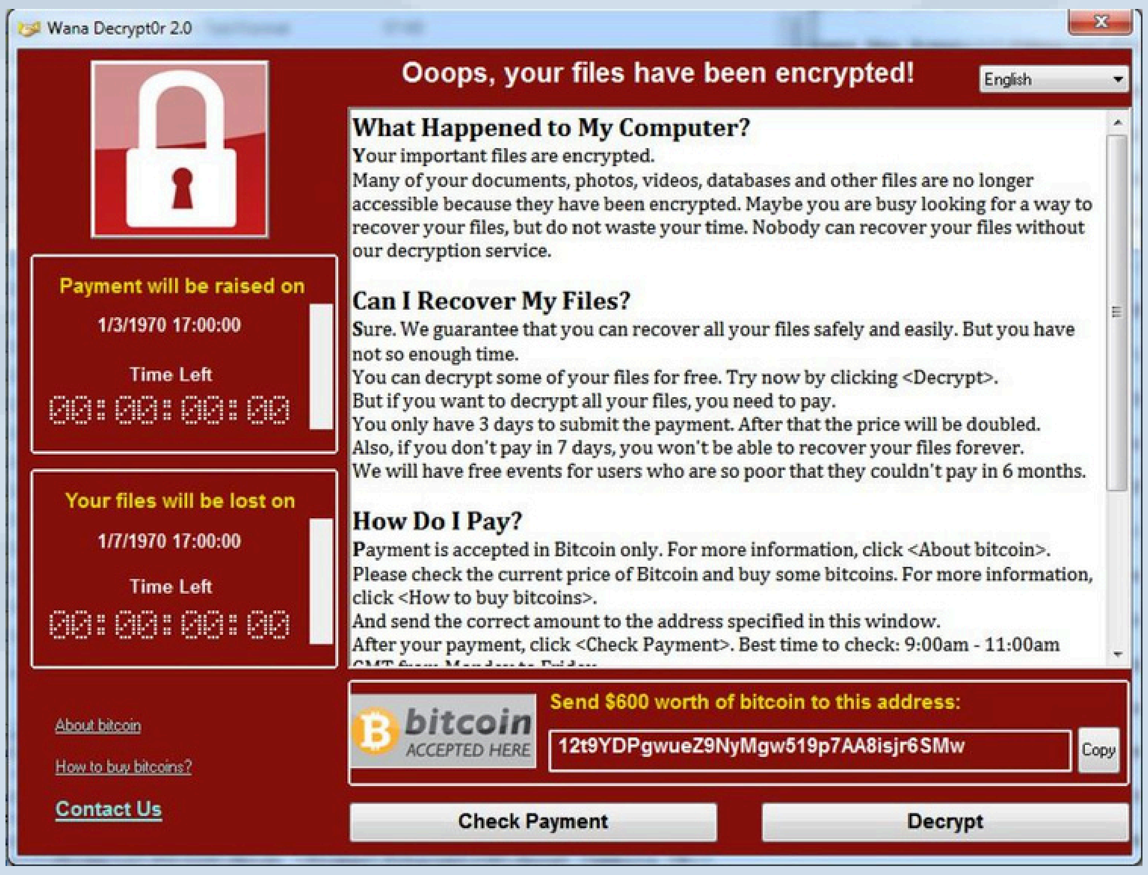
**SPYWARE** is a type of malware that works by spying on the user's activity without their knowledge. Spyware can collect user information (passwords, financial data, etc.) and monitor user activity (Internet activity, keystrokes, etc.).

**RANSOMWARE** is a piece of computer malware that stealthily installs itself on the victim's device and holds their data hostage until a ransom is paid.



The attack that happened with WannaCry ransomware in May 2017 has been reported to have infected more than
230,000 computers in over 150 countries in one day. The malware encrypted files with a ransom of $300 to
$600 to be paid in bitcoin.

Despite these multiple definitions, the characteristics and elements useful to understand what is meant by web 2 compared to web 1.0 are the following:



**What Happened to My Computer?**
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

**Can I Recover My Files?**
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

**How Do I Pay?**
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Payment will be raised on
1/3/1970 17:00:00
Time Left
00:00:00:00

Your files will be lost on
1/7/1970 17:00:00
Time Left
00:00:00:00

Send $600 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Funded by
the European Union

**SCAREWARE** is a form of malicious software that uses social engineering to provoke shock, anxiety, or perception of a threat in order to manipulate users into purchasing unwanted software. It usually suggests that users download and pay for fake antivirus software to remove it.

## THE SYSTEM INFECTION PROCESS

*What are the most common ways to infect your device with malware?* This can happen when:

- you open an email (**infected**) from unknown addresses,
- you browse unsafe sites,
- you don't update your operating system,
- you don't run the spyware scanner,
- you download infected software,
- You download pirated and unauthorized software, music, or movies.

Funded by
the European Union

# INFECTION PREVENTION

While there is no such thing as safe use of computers and the Internet these days, there are many things we can do to minimize the risk. Have you installed a commercial antivirus program on your computer and your mobile phone or tablet? Do you update it regularly? Do you have the same access code (password) for each of your network accounts? Do you use your networked accounts on all devices?

Here's what you can do to protect your computer or mobile device from viruses and other malicious software:

- ✓ Install an authorized antivirus program and update it regularly (e.g., AVG, Avast, Kaspersky, McAfee). There are also a few free options available.

- ✓ It regularly installs security updates for its operating system. Some systems can be set to automatically update at a certain time of the day/week/month. Sometimes updates take a lot of bandwidth and a lot of time to process, so it's a good idea to set them up for a time when you're not working on your device. *Why not set theAutomatic updates during Sunday lunch or maybe overnight*?

Funded by
the European Union

## ANTIVIRUS PROGRAMS

To properly combat viruses, it is always a good idea to install an antivirus program on your system. Even if you already have one, make sure it hasn't expired and that it's set to receive automatic updates. You can choose from a number of antivirus programs available, many of which are also free.

***The antivirus program you choose should have two modes:***

1. **Interactive**: In this mode, the program hides in the background and monitors the computer's activity, always looking for a virus coming from an e-mail, www, USB, etc. If a virus is detected, a message flashes on the screen.
2. **Scanning**: In this mode, the antivirus program scans and checks all parts of your computer's memory and storage system, looking for signs of infection.

Just in case, it is recommended that you set your antivirus software to scan automatically.

**Use a firewall.**
Use your browser's pop-up blocker.
Set strong passwords for your accounts.
When you are finished working, always log out of your network account on all your devices.

Funded by
the European Union

## PROTECT YOUR DEVICE FROM PHYSICAL HARM

While it seems obvious, it might be helpful to remember to keep your devices away from children and pets. Also, not eating or drinking while using your computer can avoid the risk of spilling food or drinks on the keyboard or other components. This is especially true when using a laptop because the components are all placed inside.

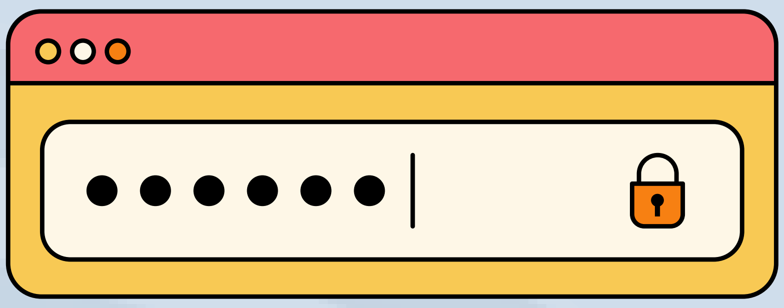
It is very important to connect your computer, screen, and router to a surge protector and prevent it from being damaged during lightning storms. In such cases, if you don't have a surge protector, you should at least disconnect the devices from the electrical system.

It would also be helpful to consider purchasing extended insurance for the devices. While it doesn't cover accidents like dropping your computer or spilling liquids on your keyboard, it could save you high repair costs.

Funded by
the European Union

# Password

The **password** or **passcode** is the first line of defense in cybersecurity.



By now, everyone should know that passwords like "123456" and "password123" are not strong enough , i.e., secure. However, there are still millions of people who don't use secure passwords.

According to password management company Keeper Security, the list of the most common passwords is simply shocking. Here is the list of the most used passwords in 2016.

1. Qwerty
2. 12345678
3. 111111
4. 1234567890
5. 1234567
6. password
7. 123123
8. 987654321
9. qwertyuiop
10. Mynoob
11. 123321
12. 666666
13. 18ATCSKD2W

Funded by
the European Union

***Have you realized that you have used passwords like this??***

Now, let's learn how to create a secure password.

Sorry, but your password must contain an uppercase letter, a number, a haiku, a gang sign, a hieroglyph and the blood of a virgin.
someecards
user card

- Mix uppercase and lowercase letters, numbers, and symbols (for example, @, #, $,%) if allowed.
- Use at least eight characters (the more characters you use, the stronger your password).
- Use the initial letters of a phrase you like, especially if a number or special character is included.
- Take two familiar things and then combine them with a particular number or character.
- It is recommended that you change your password every 3 months.
- Don't use the same password for all the accounts you're using.
- Finally, the best password is a password that is easily RECALLED.

Funded by
the European Union

## Password Manager

You have at least five online accounts such as Google, Facebook, Twitter, LinkedIn, and Instagram, plus home banking, a government portal, etc. Now that you know how to create a secure password, it's time to discover password manager software. How will you be able to use strong, unique passwords for all the websites you have access to or want to access?

The answer is password management software. Password managers like KeePass store your login information for all the websites you use and help you automatically log in to them by encrypting your password database through the use of a master password. The master password then remains the only password you need to remember.

### SECURITY OF PERSONAL DATA

## Set the privacy of networked services

Have you ever seen or changed the privacy settings for the online services you use, such as eBay, Gmail, InstaeBay, Gmail, Instagram, Facebook, Google, YouTube, etc.?

Funded by
the European Union

To achieve a certain level of security on the Internet, you need to be able to understand the correct setting for your privacy in the network services you use, and how to best manage it.

## Making browsing safer

Here are some tips on how to make your browsing safer:

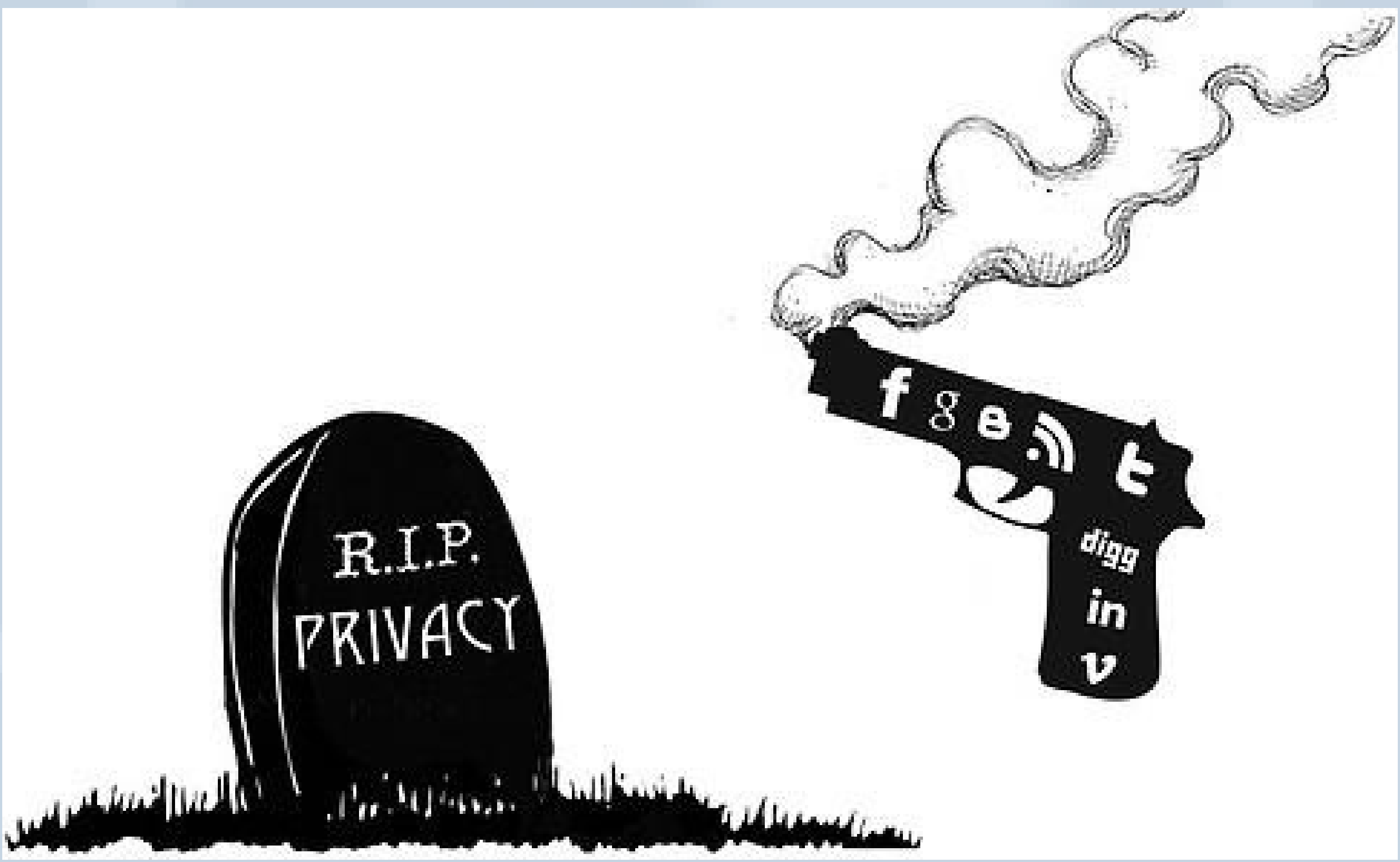
- Enable automatic updates to your search engine (browser).
- Block pop-ups, plug-ins and phishing sites.
- Set your browser so that it does not store your password.
- Disable third-party cookies.
- Depending on the browser you are using, you will need to adjust its settings for maximum security.

Funded by
the European Union

## Set social network privacy

DATA
PRIVACY

Social networks allow people to connect, but they are also a popular platform for launching online threats and cyberbullying. Unwittingly, people, especially children, often share more information online than they should. This makes them particularly vulnerable.



Recent studies have shown that 9 out of 10 teenagers post photos of themselves online or use their real names on their profiles; 8 out of 10 reveal their dates of birth and interests; and 7 out of 10 post the name of the school and the city where they live. These actions can make children easy targets for online "predators."

Privacy settings are controls available on various social networks (e.g., Facebook) and other websites that allow users to restrict access to their profile and what information visitors may see.

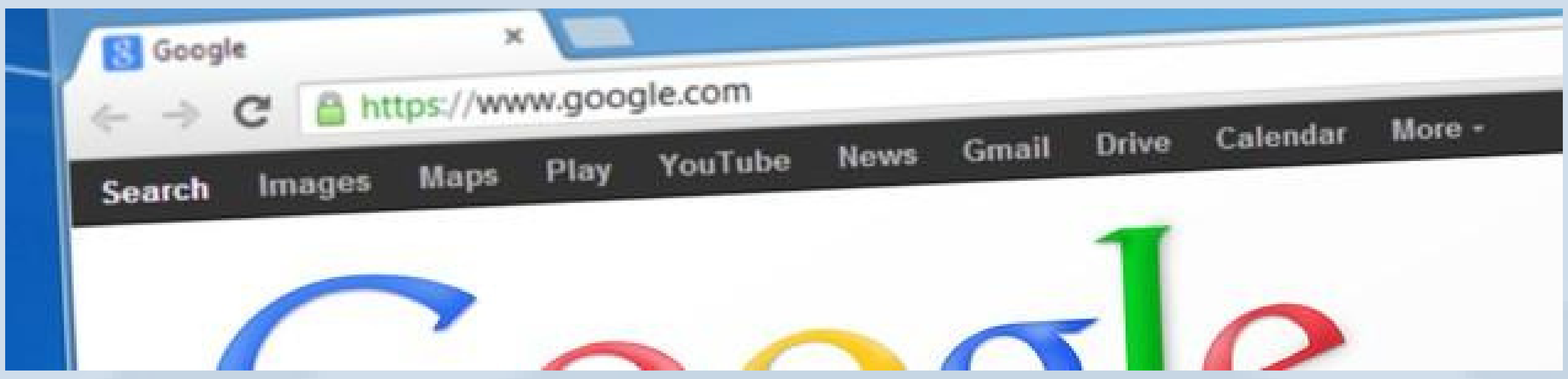
While content filtering solutions can be used to prevent pupils from accessing social media while using school computers, nowadays most students bring smartphones to school and once they connect to the internet on those devices, they are out of all possibility of control by the school. That's why it's crucial to promote responsible digital citizenship in school curricula.

## The https protocol and secure websites

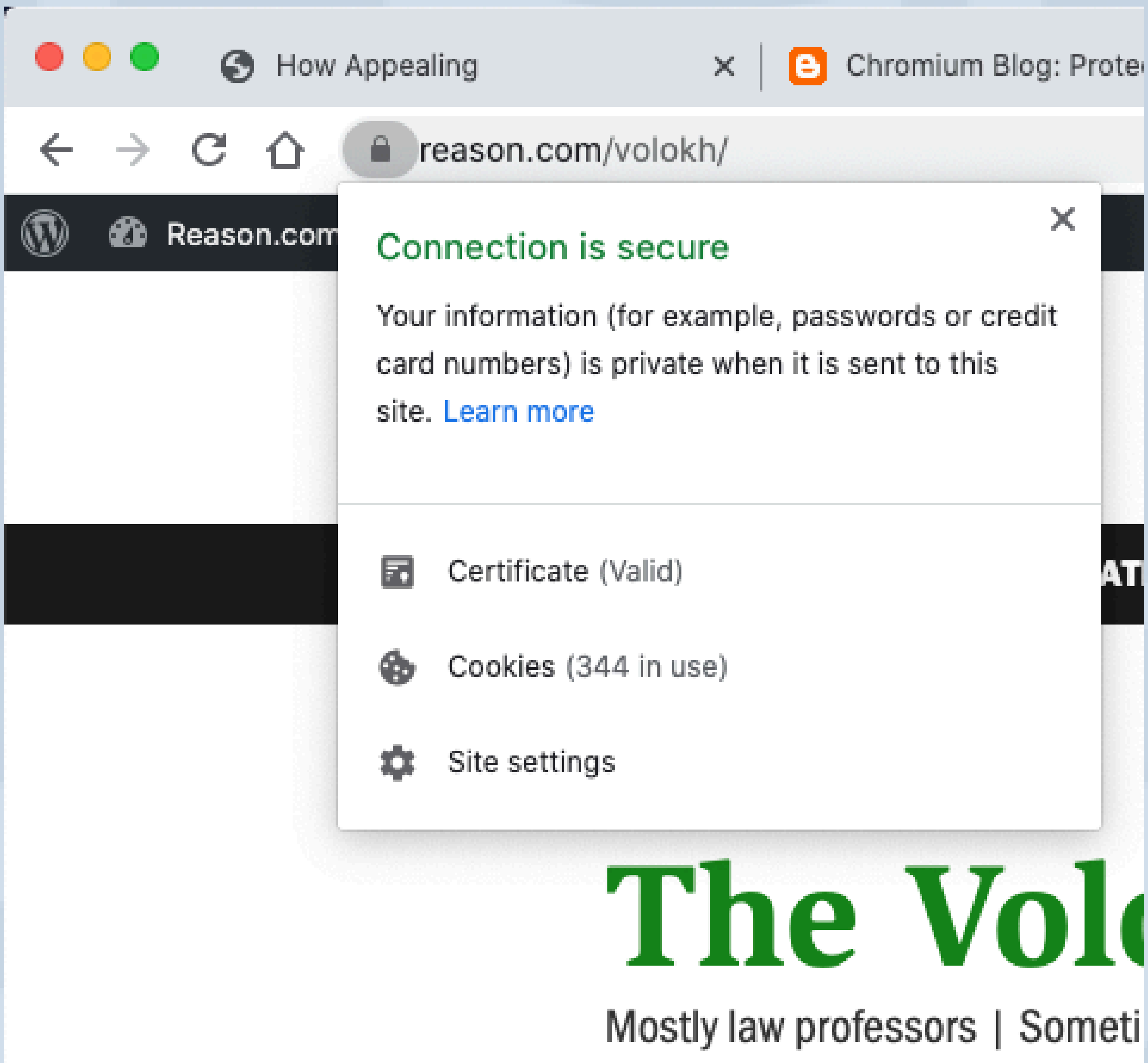
A secure website does not contain any malware programs, it encrypts all data that passes through it in order to ensure a secure exchange of personal data or financial transactions from any compromise.

Funded by
the European Union

## *How can you tell if a website is safe?*



If the website uses HTTPS (a communication protocol for secure communications over a computer network), the word HTTPS will appear before the website address.



Connection is secure

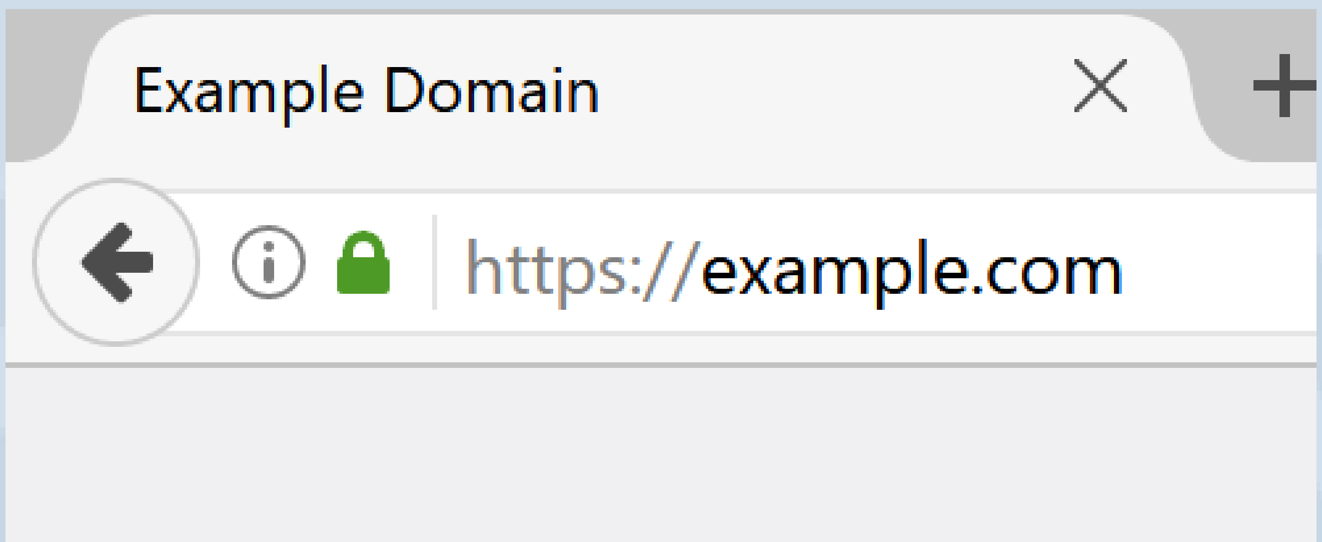
Your information (for example, passwords or credit card numbers) is private when it is sent to this site. Learn more

Get to know your browser and its features. In addition to https, an icon may appear. For example, if you use Google Chrome to check the security of a site, look at the security status on the left side of the web address.

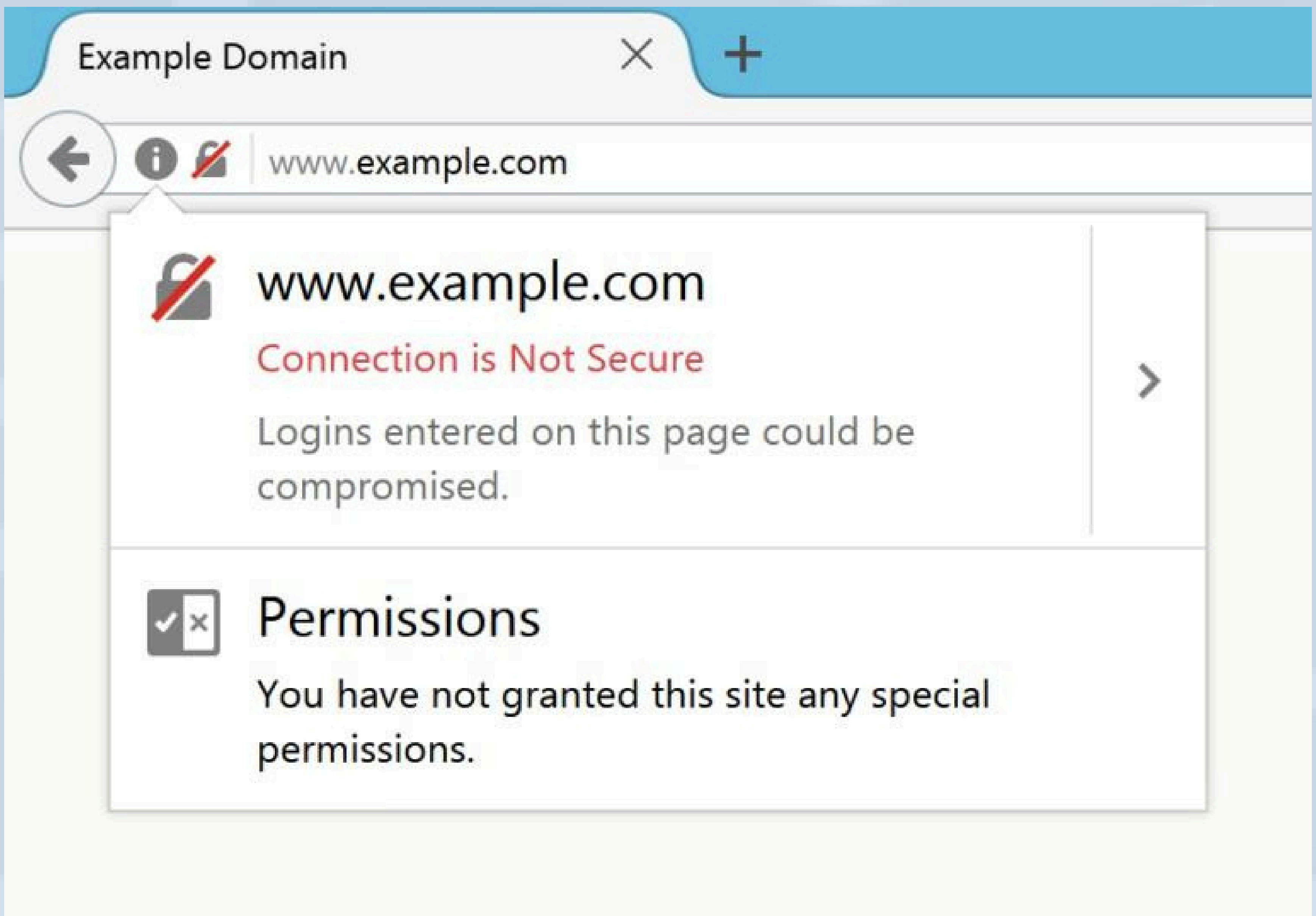
Funded by
the European Union

If you're using Firefox, the security status is also on the left side of the web address:

- Sure



- Warning



www.example.com

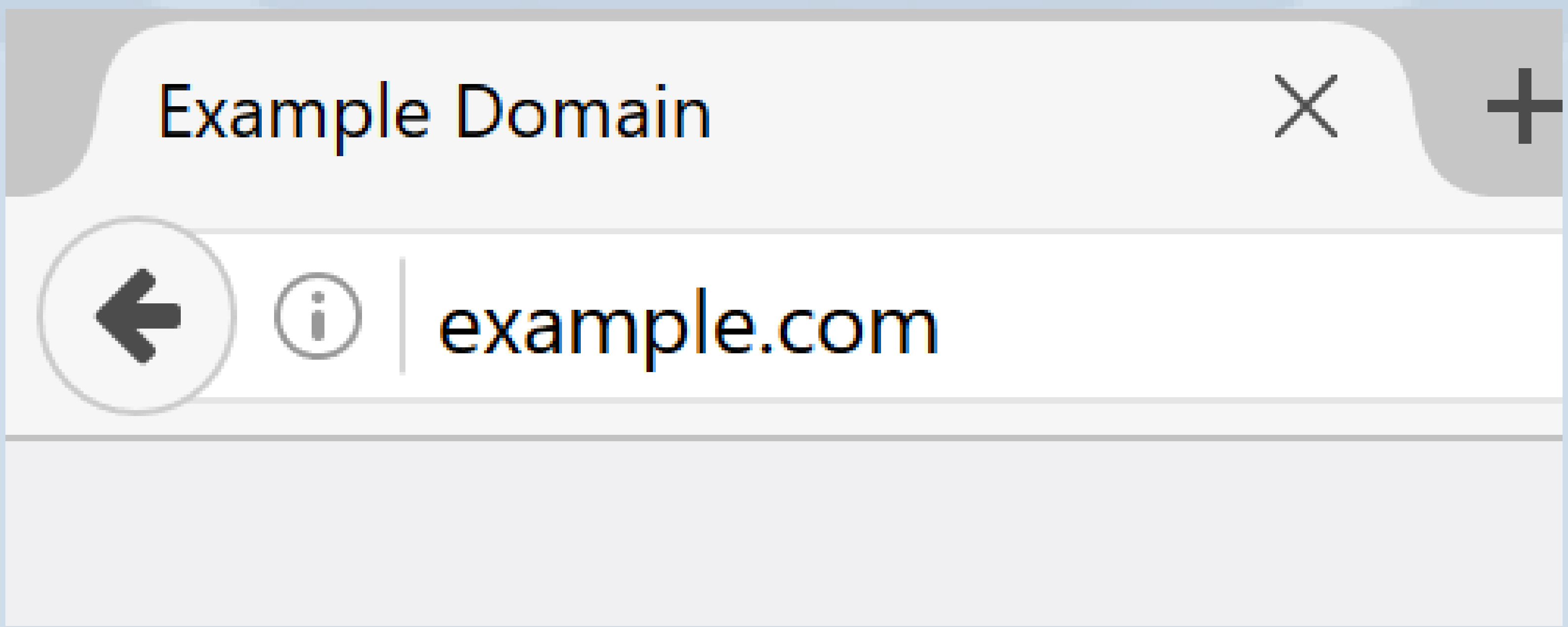
Connection is Not Secure

Logins entered on this page could be compromised.

Permissions

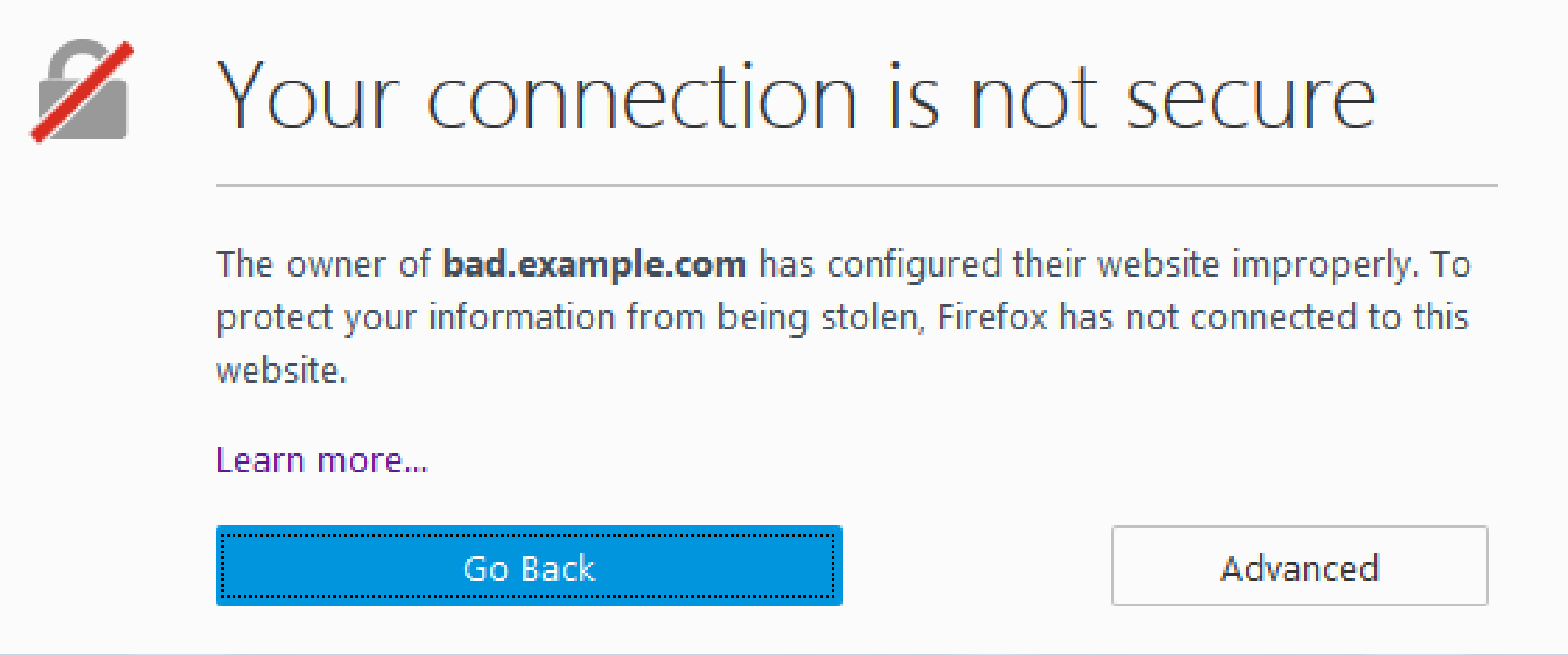
You have not granted this site any special permissions.

- Not Safe or Dangerous



Funded by the European Union

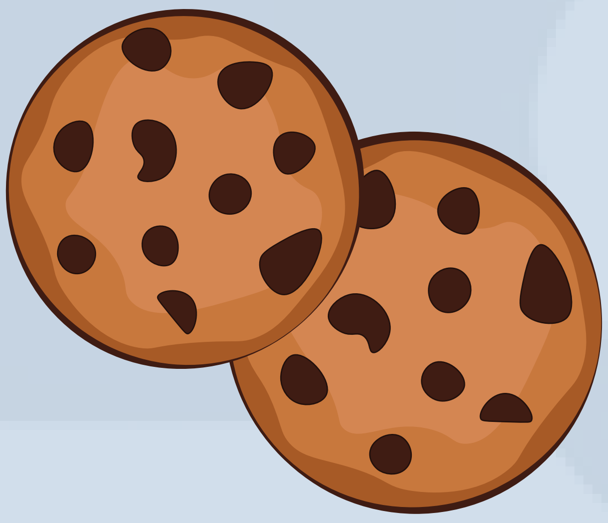
Special care should be taken when transferring sensitive and highly personal information over the network. Some websites may not be updated to the latest SSL standards, which can be dangerous for data transfer, but secure enough to browse and search for information.



Your connection is not secure

The owner of **bad.example.com** has configured their website improperly. To protect your information from being stolen, Firefox has not connected to this website.

## Cookies



Internet cookies are small files that are stored on your computer. The main purpose of a cookie is to identify users and possibly prepare personalized web pages or store site login information. Cookies usually do not contain sensitive or highly personal information or anything dangerous. In most cases, this means that the website remembers your username. If you delete your cookies after visiting a particular website, you will not be treated as a returning visitor. (For example, you'll need to enter their username again.)

Funded by
the European Union

## Surfing on a computer for public use

When using public computers, such as in libraries, Internet cafes, airports, hotels, etc., you need to be very careful. To keep your professional, personal, or financial information private, we recommend following a few simple rules:

- Don't ask a public computer to remember your password.
- Check if the Windows firewall is turned on and if an antivirus program has been installed.
- Do not download confidential documents to a public computer.
- Delete any downloaded content from emails.
- Log out after using any website that requires you to log in (e.g. Gmail, Facebook, LinkedIn, etc.).

Funded by
the European Union

- While entering your password and financial details on a web page, always make sure to do the following:

- Check if the address bar has "https" and a block in the URL.

- Use private browsing mode (for example, if you're using Google Chrome, in the upper-right corner of your browser window, click the Chrome menu, then select "New Incognito Window").
- Private browsing will allow you to browse the internet without saving any information about what sites and pages you've visited, but it won't make you anonymous on the internet. This means that your internet service provider (at home), employer (at work), or the sites themselves can still keep track of the pages you've visited. Private browsing won't protect you from malicious software that may be installed on your computer.

Funded by
the European Union

## Surfing a public network

We've all seen signs like this in a bar, restaurant, public buildings, etc.

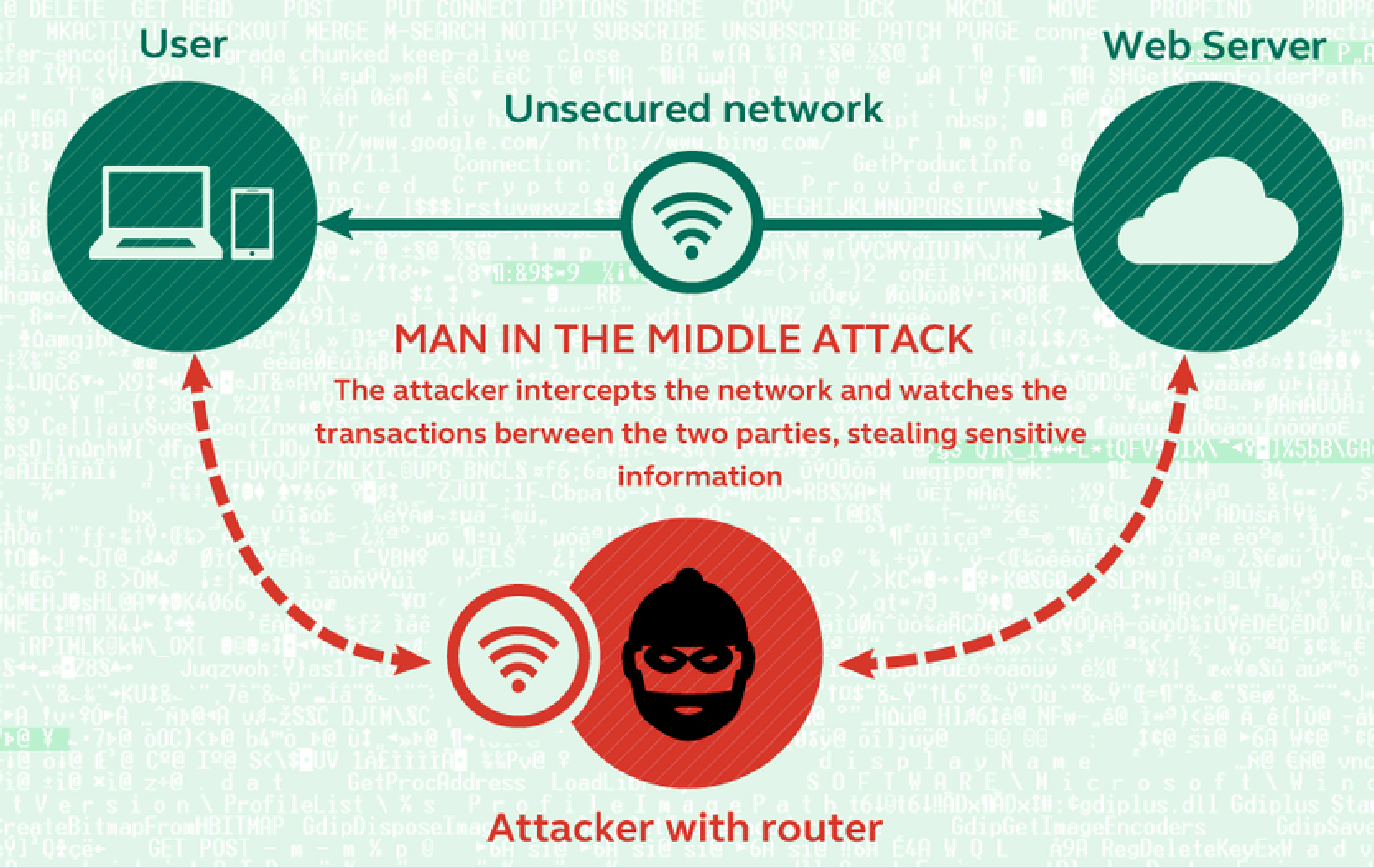
*Have you ever connected to a network like this while using your laptop, tablet, or smartphone? Were you able to connect without a password? You couldn't check if the address started with https://?* If you answered these questions with **YES**, you have potentially put your personal information at risk.

Funded by
the European Union

IAll those signs in the places should actually be replaced with this:

***What makes a wireless connection more susceptible to exploitation?***

When you connect to a public network, it's almost like inviting a stranger into your home – you trust them based on the information you have. Anyone who accesses the same (unsecured) network can intercept any passage of information between your device and the web servers.


User
Web Server
Unsecured network
MAN IN THE MIDDLE ATTACK
The attacker intercepts the network and watches the transactions berween the two parties, stealing sensitive information
Attacker with router

Funded by
the European Union

### *How to stay safe?*

SAFETY FIRST

While there are no guarantees, you can follow a few steps to minimize your risk:

- **Don't** connect to networks that don't require passwords. An official Wi-Fi network should establish a password. For example, if you're in a coffee shop, ask the staff to check what their network is. There may be a fake net specially set up under the same name as the bar.
- **Don't** connect to websites that don't use HTTPS.
- **Don't** connect to public networks to use your credit card, check your bank account, pay bills, etc.

- When you're done browsing using their Wi-Fi, **be sure to disconnect** and remove the network so it doesn't automatically connect you the next time you're back in the venue.
- **Turn on Wi-Fi only when you really need it**. This will prevent your device from automatically connecting to random networks.

Funded by
the European Union

## Secure use of cloud storage

WHAT A GREAT IDEA TO STORE EVERYTHING IN THE CLOUD! I'LL START GETTING STUFF DOWN FROM THE ATTIC.
© D.Fletcher for CloudTweaks.com

Storing your files (e.g., images, videos, music, documents, etc.) in cloud storage (e.g., Google Drive, Dropbox, iCloud, Box, etc.) has many advantages, for example, there is a lower risk of losing data. Files stored in the cloud can be easily viewed from your computer and a mobile device connected to the internet.

Although storage companies normally take the necessary security measures, there are no guarantees. However, hackers are very likely to acquire your data due to human error or negligence, simply by cracking your password. So you should always make sure to:

- use a strong and secure password,
- change your password regularly,
- Don't store personal information in the cloud
- If possible, create a backup copy on another device (e.g., an external hard drive).

Funded by
the European Union

# Digital footprint: monitoring identity on the network

A digital identity (digital footprint) is the online representation of an individual within a virtual world such as a chat room, forum, video game, or virtual communal space. All online activities (browsing, blogging, posting on social media and forums, signing online petitions, etc.) leave a trace, the so-called digital footprint.

# Guidelines for protecting your online identity

*Have you ever Googled your name?* Have you ever found something you wouldn't want others to see? You should protect your "brand on the net" and follow these rules:

- Use networked tools to build a positive footprint.
- Never post anything you might regret in the future.
- Be respectful of yourself and others.
- Choose appropriate usernames and avatars.

Funded by
the European Union

- Imagine what family and friends might think if they saw what you're doing online.
- Block those users who reflect little on their reputation.
- Trace information about yourself.
- Make sure that your friends only use your image with your permission, and vice versa.
- Think before you click.
- Monitor your digital identity and fingerprints to protect against online fraud and i dentity theft. Think about how he would like to be seen.

## Manage multiple identities on the network

We have just mentioned that a digital identity is the networked representation of an individual within a virtual world such as a chat room, forum, video game or virtual common space. People construct digital identities as virtual representations of themselves for various purposes (anonymous, professional, educational, personal).

Funded by
the European Union

- Here are some benefits of using multiple digital identities:
- A digital identity allows you to create anonymous profiles and blog or chat anonymously.
- You can stay private and yet explore various opportunities.
- You can build a positive digital identity for professional opportunities (e.g., LinkedIn).
- You can create a digital identity for educational purposes.

*How many digital identities do you have? How do you manage them? Have you already learned about password management software? (e.g. KeePass).*

## Protect yourself from online fraud and identity theft

You've already learned about various methods that can help you protect your personal data on the internet, such as how to recognize a secure website, use the internet on a public computer, safely use cloud storage, and track identity and fingerprints. Now you will learn how to protect yourself from online fraud and identity theft.

Funded by
the European Union

Here are some simple rules you should follow, many of which you have already learned in previous topics:

- Protect your computer and mobile device with strong and up-to-date anti-malware software.
- Use strong passwords.
- Have different passwords for each account.
- Tracking down information about yourself – looking at what private information can be viewed by others.
- Monitor banking and credit card communications.
- Use HTTPS whenever possible.
- Recognize suspicious emails and attachments.
- Think carefully every time you enter your personal information online.

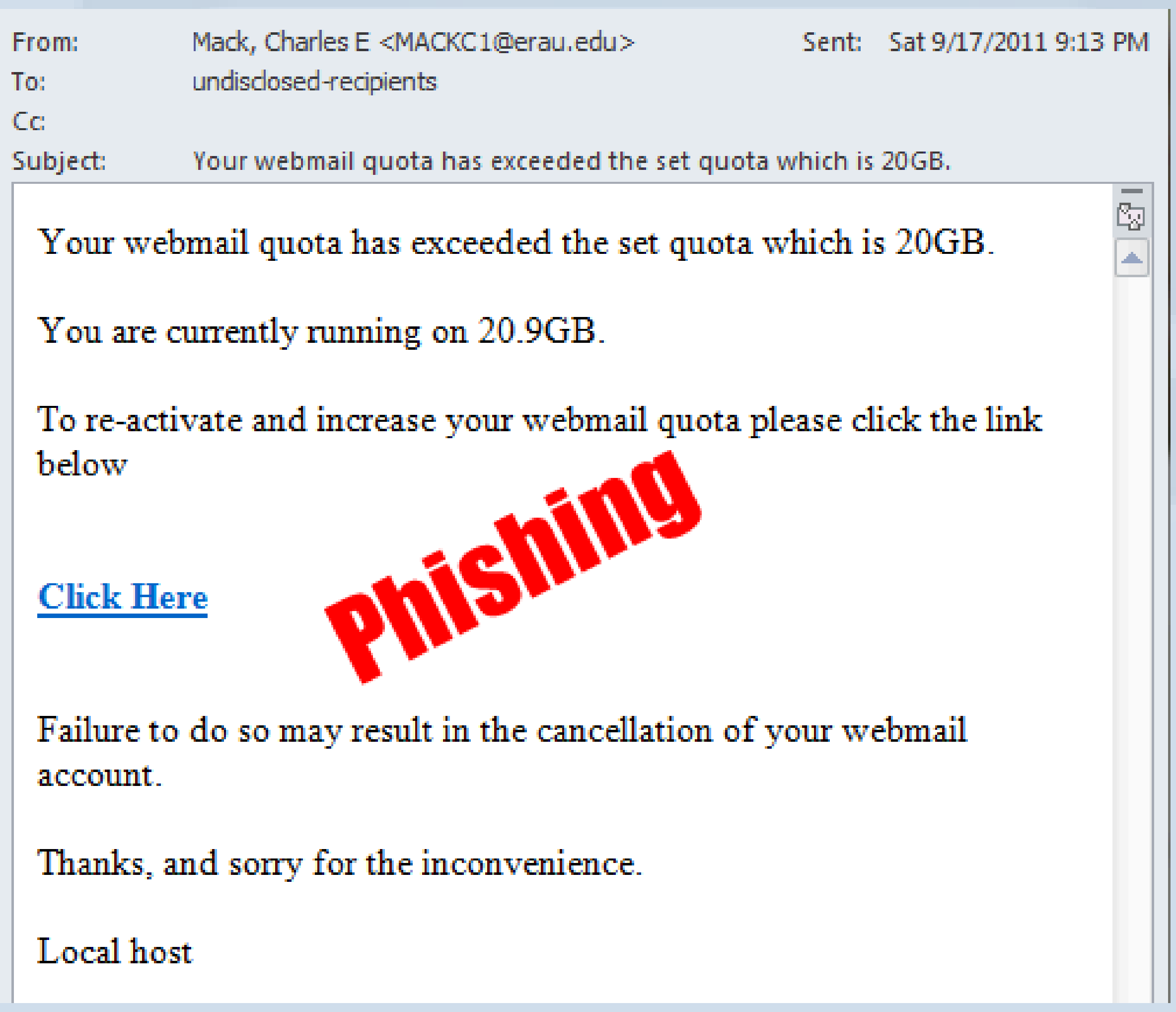
Funded by
the European Union

# Phishing

*Phishing is defined as attempting to obtain sensitive information such as usernames, passwords, and credit card details, often for malicious reasons, by posing as a trusted entity in electronic communication.*

Phishing is typically done through spoofing or instant messaging of email messages, and often directs users to enter personal information on a fake website, the appearance and format of which are almost identical to legitimate ones. Communications purporting to come from social networking websites, auction sites, banks, networked payment processors, or IT administrators are often used to lure victims. Phishing emails may contain links to malware-infected websites.

Here's an example of a phishing attempt that attempts to obtain users' email information.



From: Mack, Charles E <MACKC1@erau.edu>  Sent: Sat 9/17/2011 9:13 PM
To: undisclosed-recipients
Cc:
Subject: Your webmail quota has exceeded the set quota which is 20GB.

Your webmail quota has exceeded the set quota which is 20GB.

You are currently running on 20.9GB.

To re-activate and increase your webmail quota please click the link below

Click Here

Failure to do so may result in the cancellation of your webmail account.

Thanks, and sorry for the inconvenience.

Local host

Funded by
the European Union

# How to Identify Phishing Scams

Here are some tips on how to identify email phishing scams:

- Don't trust the name displayed on the screen.
- Look but don't click.
- Check for spelling mistakes.
- Analyze the form of greeting.
- The message asks for personal information.
- Be wary of urgent or threatening language in the subject line of the message.
- Review the signature.
- Don't click on attachments.
- Don't think the sending address is the one listed in the header.
- The offer seems too good to be true.
- The message appears to come from a government agency.

Funded by
the European Union

# Cyber bullying

The internet has opened up new possibilities for all of us. The other side of the coin, however, is represented by the risks associated with improper use of this tool: among these is cyberbullying.

Cyberbullying can be defined as the use of new technologies to intimidate, harass, embarrass, make others feel uncomfortable, or exclude them.

For young people who are growing up in contact with new technologies, the distinction between online and offline life is very minimal. The activities that children carry out online or through technological media therefore often have consequences in their real lives as well. In the same way, online lives also influence the way children behave offline, and this element has several repercussions that must be taken into account in order to fully understand cyberbullying.

Funded by the European Union

All this can be done using different modalities offered by new media. Some of them are:

- Phone calls
- Messages (with or without images)
- Synchronous chats
- Social networks (e.g., Facebook)
- Q&A Sites
- Online Gaming Sites
- Online Forums

There are many specific ways in which children engage in cyberbullying. Some examples are:

- gossip spread through messages on mobile phones, emails, social networks;
- posting or forwarding embarrassing information, images, or videos (including false ones);
- stealing the identity and profile of others, or fabricating fake ones, in order to embarrass or damage the victim's reputation;
- insulting or mocking the victim through messages on their mobile phone, email, social networks, blogs or other media;
- making physical threats to the victim through any media.

**These aggressions can follow episodes of bullying (at school or more generally in places where children gather) or be online-only behaviors.**

Funded by
the European Union

Cyberbullying might seem harmless, but if it is not addressed appropriately, it can have serious emotional consequences for children and teens.

Here are some steps to follow to avoid cyberbullying:

- Teach children not to post personal information or anything very private.
- Explain to them not to respond with anger and resentment to a message that in turn also expresses anger.
- Explain to children why they should not open messages sent by strangers.
- Remind them to change regularly and use different access codes (passwords).
- Because these settings tend to change, it's always a good idea to update your privacy settings for networked services from time to time

### HEALTH & GREEN IT

## Know the potential health risks when working at the computer

When used correctly and in moderation, computers should have no impact on most people's health. However, intensive computer use can cause occasional, long-term health problems.

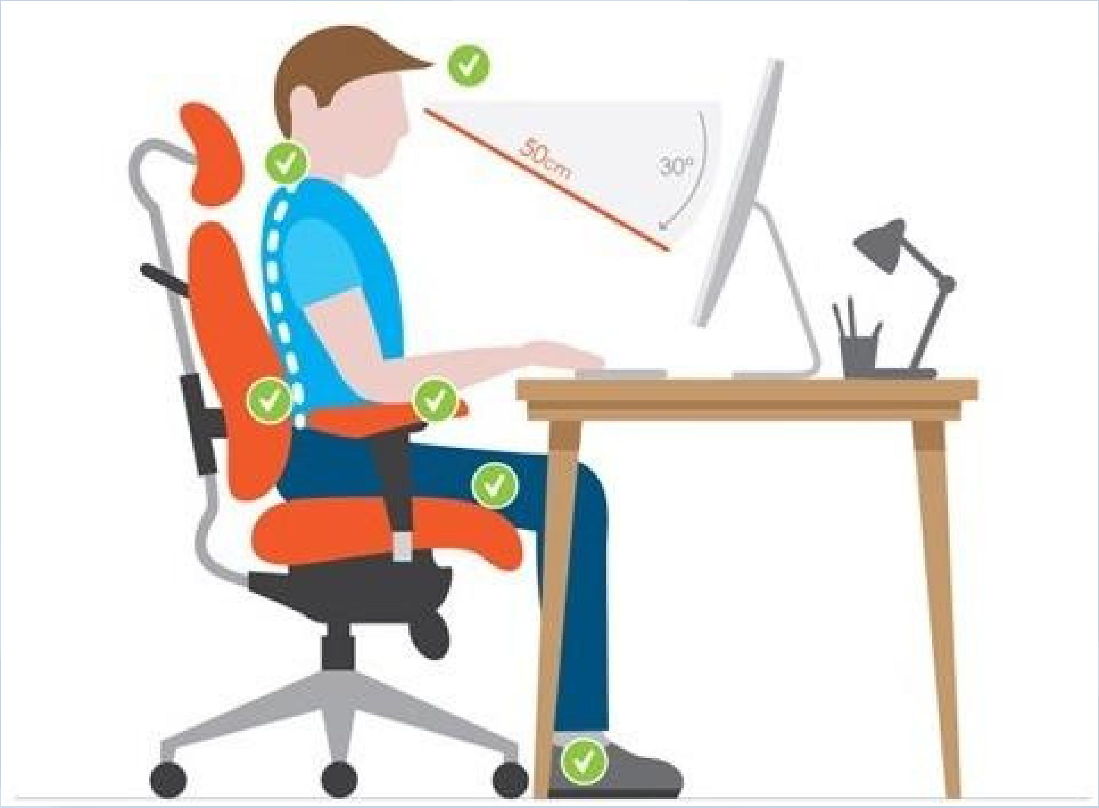
Funded by the European Union

The most common problems and complaints are:

- upper limb disorders (may affect the fingers, hands, arms or shoulders),
- back and neck pain,
- eye problems,
- stress from headaches or fatigue.

Typing for hours each day is more likely to cause repetitive strain injuries (RSIs). These types of problems can be caused by:

- unnatural or unhealthy posture when using the computer (especially laptops due to small screens, keyboards, and built-in pointing devices (such as a small mouse or portable touchpad),
- inadequate lower back support,
- sitting in the same position for a long period of time
- Ergonomically poor workstation.



Given that computers are an essential tool in our daily lives and that they can cause health problems, you need to learn how to reduce the health risks from prolonged computer use.

Funded by
the European Union

# Using the computer in a healthy way

Various measures should be applied to reduce the health risks resulting from prolonged use of the computer. Here are some examples:

- The screen image should be clear, fixed, and free of glare and/or reflections.
- The keyboard should be positioned correctly to support your wrists.
- To prevent the consequences of prolonged mouse use, it is recommended to have breaks during mouse activity.
- The work chair should provide a comfortable working position and should be fully adjustable. It should be adjusted so that users' forearms are positioned horizontally and the top of the screen is at eye level. A footrest can also be used.
- Alongside these physical arrangements, regular changes in working positions as well as regular periods of rest from staring at the screen are essential to avoid computer-induced health problems.

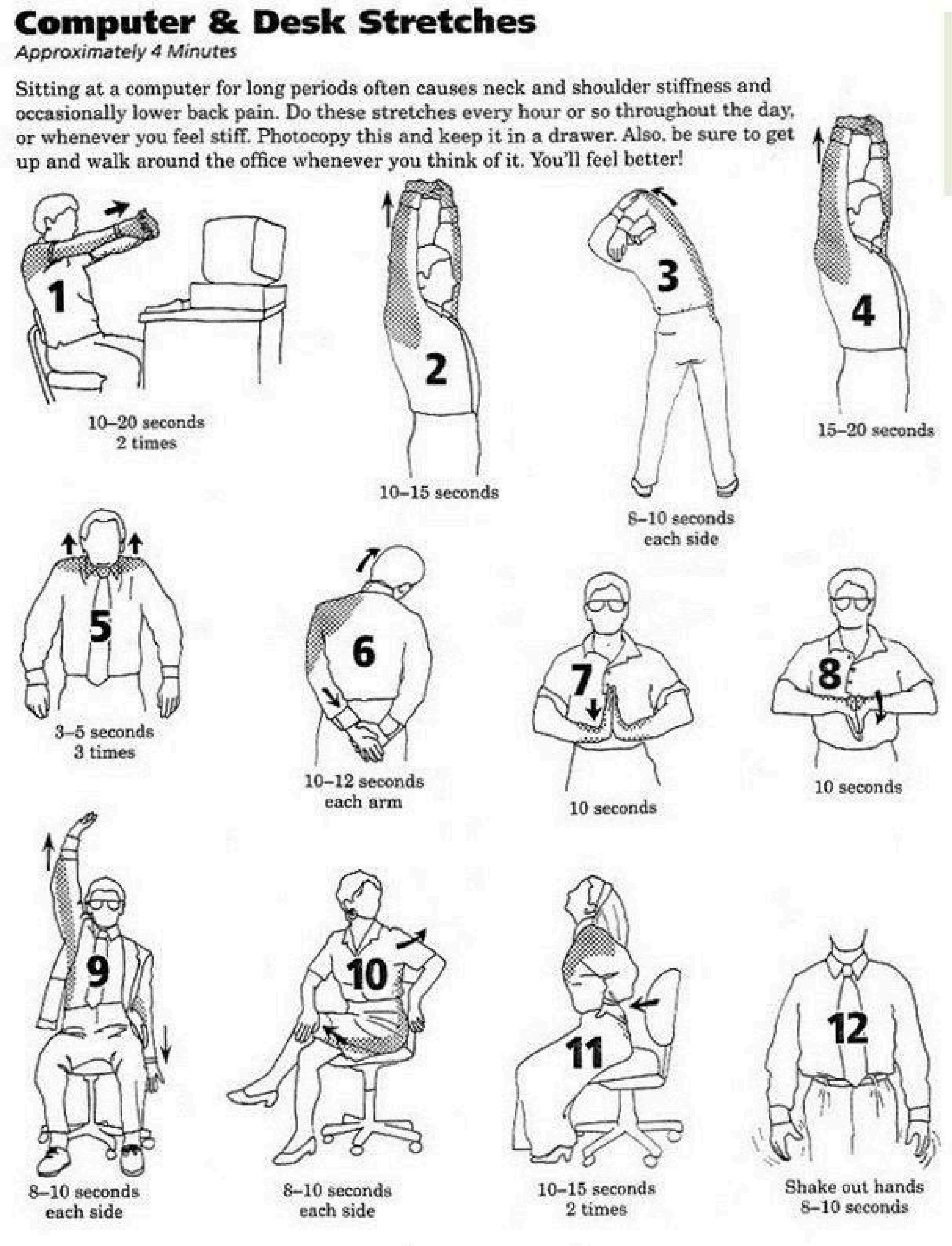
Clear indications on how to use computers in a healthy way can be found in the directives of the European Agency for Safety and Health at Work Directive 90/270/EEC

Funded by
the European Union

# How to relax your muscles while working on the computer

You have already learned that computer use can cause health problems and ways to reduce health problems with the use of proper equipment, ergonomic workplace design, and following specific work practices (regular changes in work positions and regular periods of screen rest).

In order to improve your posture and keep your health in check, you will now explore how to relax your muscles when working all day on the computer.



**Computer & Desk Stretches**

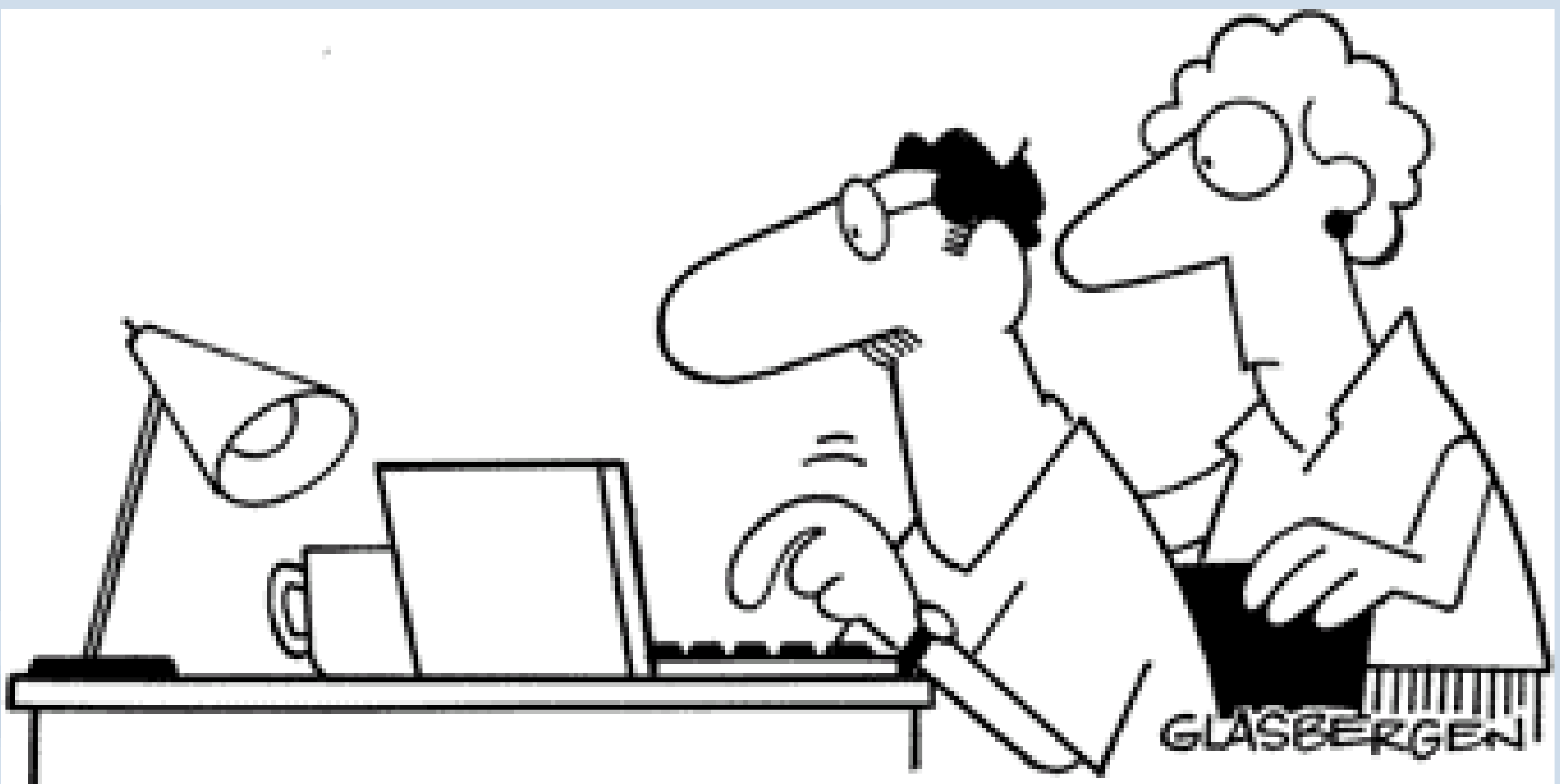
*Approximately 4 Minutes*

Sitting at a computer for long periods often causes neck and shoulder stiffness and occasionally lower back pain. Do these stretches every hour or so throughout the day, or whenever you feel stiff. Photocopy this and keep it in a drawer. Also, be sure to get up and walk around the office whenever you think of it. You'll feel better!

The American National Institutes of Health (NIH) provides a comprehensive list of various exercises and traits such as eye and musculoskeletal exercises, warm-up for work, back exercises, aerobic exercises, and recommendations for rest of the back muscles.

Funded by
the European Union

## Finding balance between online and offline life



"Dear Andy: How have you been? Your mother and I are fine. We miss you. Please sign off your computer and come downstairs for something to eat. Love, Dad."

We are surrounded by technology. The Internet has changed the way people interact. Nowadays, to communicate, we prefer to use e-mail, instant messaging (IM) and social networking sites. While work collaborations have never been easier, it seems that most people have replaced their offline social lives with online ones. Networked interactions can hardly replace face-to-face interactions, and the more time we spend socializing online, the less time we have to socialize offline, i.e., off-network, in the real world. While it's more convenient to stay connected online, strive to strike a balance between the online and offline worlds, and don't let online interactions replace time spent offline with friends or family.

## ICT devices - the new for the old

The technology used in ICT devices such as mobile phones, smartphones, tablet PCs, laptops, televisions, computer screens, gaming stations, and storage devices changes very often.

Funded by the European Union

# ICT devices - the new for the old

The technology used in ICT devices such as mobile phones, smartphones, tablet PCs, laptops, televisions, computer screens, gaming stations, and storage devices changes very often.

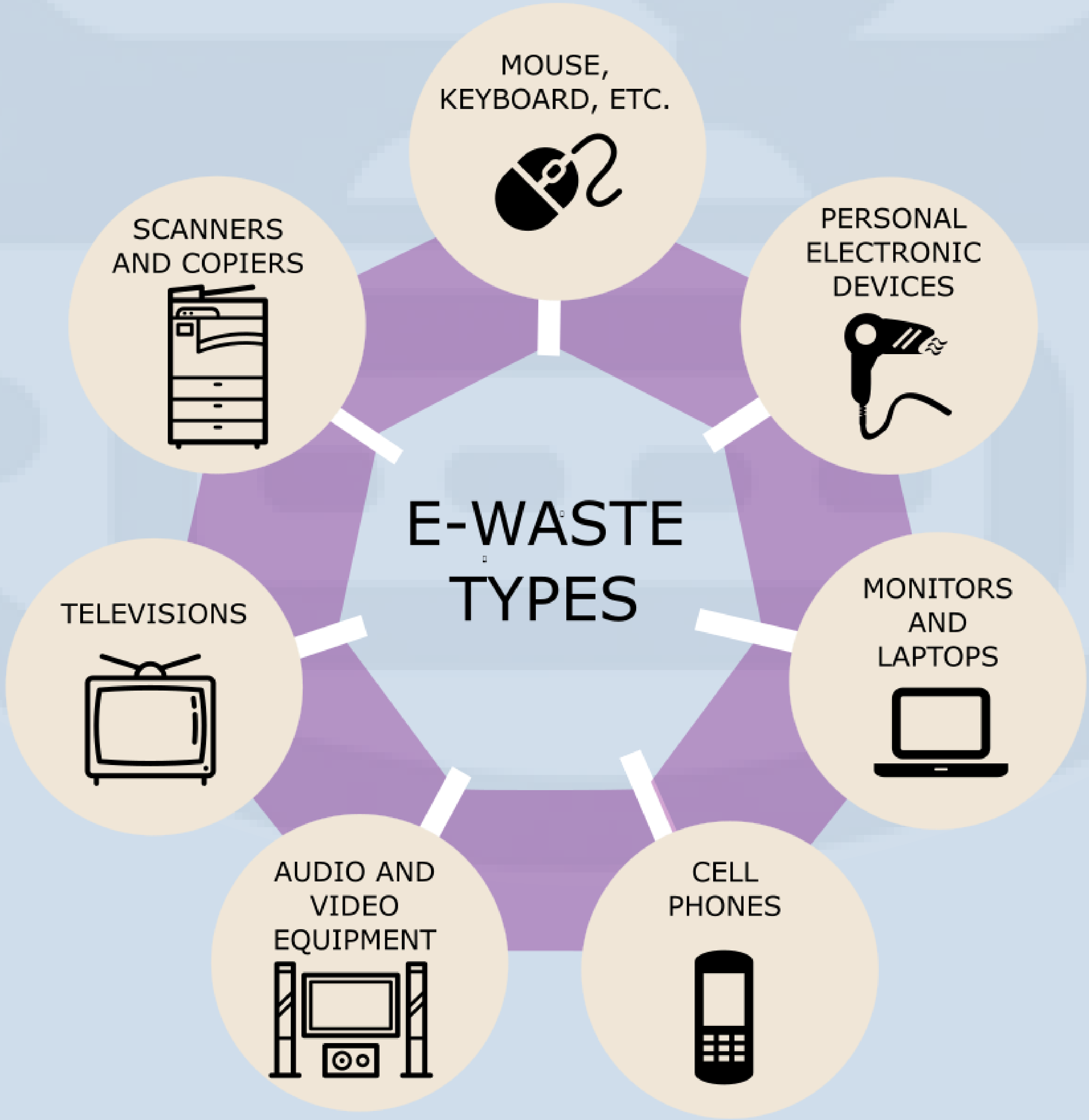
Electronic devices that were heavily used by users a year ago have now become old and obsolete. Even though the "old" devices still work fine, people throw them away and replace them with new ones.

Our obsession with having only the most current electronic devices and throwing away outdated versions even though they still work is an example of our "disposable" society.

Funded by
the European Union

## E-waste

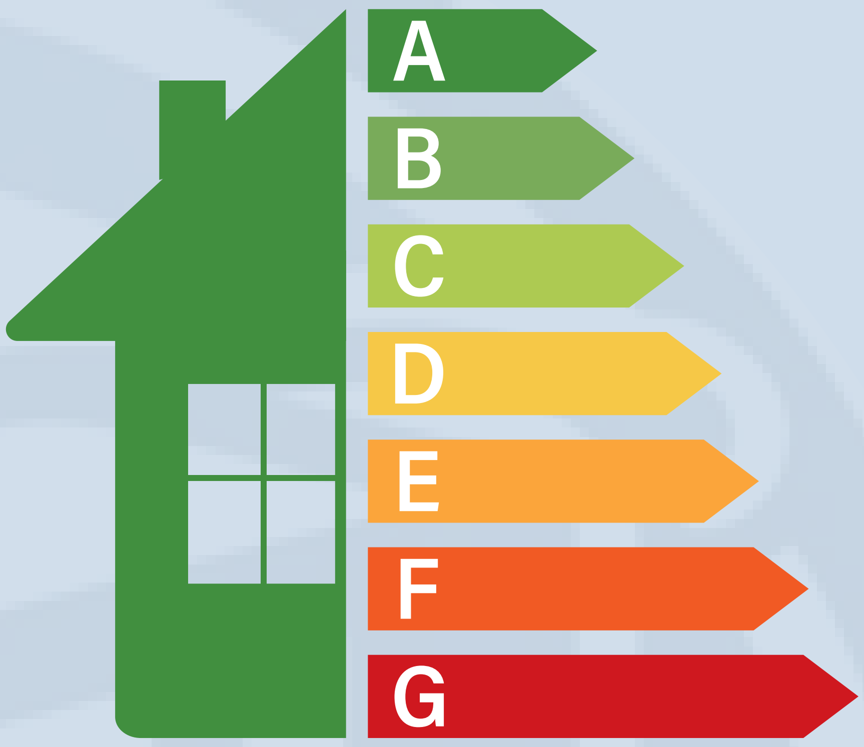
E-waste is becoming a huge problem around the world because even today, many electronic devices end up in inadequate landfills. When e-waste is not disposed of properly, toxic metals, such as lead (found in CRT screens, batteries), cadmium (NiCd rechargeable batteries, fluorescent layers of CRT screens, printer inks and toners), mercury (fluorescent lamps that provide backlighting in LCDs, some alkaline batteries, and switches in contact with mercury), arsenic (inside light-emitting diodes), and beryllium (power boxes that contain rectifiers and silicon-controlled X-ray lenses) are absorbed by the soil and can contaminate drinking water.



Funded by
the European Union

This is why most countries have introduced very strict regulations to prevent e-waste from being dumped in inappropriate landfills. While there are strict regulations, some countries have sent their e-waste to places like Asia, where such laws are not as strict.

## Green IT and energy efficiency



E-waste is filled with valuable materials such as gold, nickel, steel, lead, copper, and plastic. Each of these materials can be reused. For example, the zinc contained in mobile phones could be used in shipbuilding or for galvanizing metal railings and lampposts. The gold contained in video game consoles can be turned into jewelry. Plastic can be reused to make musical instruments.

There are three key factors when thinking about recycling, namely the **3 R's:**

1. reduce the amount of waste that is produced
2. reuse everyday objects
3. recycle.

Funded by
the European Union

We need a large amount of electricity to power millions of ICT devices around the world. Due to the way electricity is generated, the use of electronic devices contributes to global greenhouse gas (GHG) emissions, however, ICT devices can also be used to reduce energy consumption.

For example, many modern buildings have digitized systems for environmental control. In fact, it is often a computer that controls the air conditioning system, automatic gate openers and solar filters to control the effect of sunlight and cool the building, solar panels to reduce electricity consumption, energy monitoring displays, energy-efficient LED lighting controls and water reuse systems, especially in factories.