HOW CAN I PROTECT MYSELF ONLINE?

BEST PRACTICE TO CREATE A PASSWORD

Email, social networks, banks, government websites, online shopping, business networks and applications – the list goes on. Security for these everyday services is usually based on passwords.

Protect your accounts by following best practice.

→ USE A SUFFICIENTLY LONG AND COMPLEX PASSWORD

• **10 characters minimum**
Length is an important feature of your password.

• **Containing all the following character types:**

→ Numbers *(012...9)*
→ Lowercase letters *(abc...z)*
→ Special characters *($*%'&)*
→ Uppercase letters *(ABC...Z)*

→ USE A DIFFERENT PASSWORD FOR EACH SERVICE

→ USE A PASSWORD THAT IS IMPOSSIBLE FOR OTHERS TO GUESS

→ DON'T LEAVE YOUR PASSWORD ANYWHERE

Sticky notes, notepads, shared devices and web-based email accounts are not secure places to store your passwords.

→ TURN ON "STRONG AUTHENTICATION" ON YOUR SENSITIVE ACCOUNTS WHEREVER POSSIBLE

Also called "multi-factor authentication" or "two-step authentication".

EVERYDAY HINTS AND TIPS:

Can't think of a way to create a different complex and unguessable password for each service?

→ USE A PASSPHRASE

A passphrase is a strong password based on a phrase:
• **Choose a phrase that you can remember easily.**
• **Use the first letter of each word** to create your password.
• **The phrase must contain figures and special characters** such as uppercase letters, punctuation marks or special characters ($, #, etc.) and at least ten words.

Example of passphrase creation:

The Olympic and Paralympic Games of Paris 2024 make the Games wide open! → TO&PGoP2024mtGwo!!

Phrase — Associated password*

** Don't use this password as it has been made public – choose a phrase personal to you to create your own password.*

→ ONE PASSWORD TO RULE THEM ALL

Use a password manager to securely store your passwords. You will then only need to remember one strong password to access all your accounts. It is not recommended to mix professional and personal passwords in the same password manager.

To find out more:
ENISA – Basic security practices regarding passwords

HOW CAN I PROTECT MYSELF ONLINE?

IDENTIFY A PHISHING ATTEMPT (EMAIL / TEXT / CALL)

Phishing is a fraud technique designed to trick an Internet user into revealing sensitive personal data (usernames, passwords, etc.) or bank details by impersonating a trusted third party. This can take the form of a fake email, text message or phone call supposedly from an everyday service: banks, social networks, mobile phone operators, energy suppliers, online stores, government agencies, etc.

Protect your data by following best practice.

➜ NEVER DIVULGE SENSITIVE INFORMATION

Paris 2024 will never ask for your password. Paris 2024 will never ask for your bank details except at your request.

➜ CHECK THE EMAIL SENDER

Any unsolicited email from an unfamiliar email address should be handled carefully, even if it seems legitimate.

If in any doubt, go directly to the official website.

➜ CHECK THE MESSAGE CONTENT

A phishing email or SMS is unsolicited and often seems to be about a tempting offer, urgent requirement or imminent threat.

Never respond to these requests. If in doubt, check the information separately yourself with the service concerned.

➜ NEVER CLICK A SUSPICIOUS LINK

Before you click a link in an email or text message, check that the destination URL is legitimate.

If in any doubt, instead go directly to the official website.

➜ NEVER OPEN ATTACHMENTS IN SUSPICIOUS EMAILS

If you receive an unsolicited email with suspicious content asking you to open an attachment, carry out the checks listed above before opening any attachment to keep your device secure.

If in any doubt, contact the service concerned.

To find out more:
ENISA – Phishing / Spear phishing

HOW CAN I PROTECT MYSELF ONLINE?

IDENTIFY A LEGITIMATE WEBSITE

Motivated by financial gain, cyber criminals are redoubling their efforts and will not hesitate to create websites that spoof everyday services such as web-based email, online shopping, banks and government agencies.

While browsing the Internet, you should make absolutely sure that the websites you visit are legitimate. Sensitive transactions should only be made from official websites.

Browse the Internet securely by following best practice.

➜ KEEP YOUR INTERNET BROWSER UPDATED

Leading Internet browsers (e.g. Chrome, Firefox, Safari) now alert Internet users when a connection is unsafe.
Do not visit websites that your browser considers unsafe.

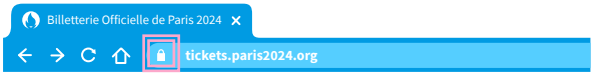
➜ CHECK THE CONTENT QUALITY

The quality of the content on a malicious website is often dubious: spelling mistakes, functions that don't work, missing content, etc.

➜ CHECK THE WEBSITE URL ADDRESS DISPLAYED IN YOUR BROWSER

If in any doubt, follow the three verification steps below:

PROTOCOL



Look for https in the URL or the padlock symbol.
If you come across a website not using the secure https protocol, it is highly likely that the website is not legitimate.
Never make sensitive transactions where the secure https protocol is missing.

DOMAIN NAME

Check that the domain name matches the official website. Official Paris 2024 websites use the domain name "paris2024.org".

DO NOT CONFUSE THE SUBDOMAIN OR PATH WITH THE DOMAIN NAME

- The **subdomain** is located just before the domain name. It is separated from the domain name by a dot (.)
- The **path** starts after the first slash (/) after the domain name.

Example breakdown of a URL:

✓ **Genuine URL:** https://tickets.paris2024.org/test

Protocol	*Subdomain*	*Domain name*	*Path*
https://	**tickets.**	**paris2024.org**	**/test**
Secure communications		*The domain name here is indeed the official website: paris2024.org*	

× **Malicious URL:** https://paris2024.tickets.org/test

Protocol	*Subdomain*	*Domain name*	*Path*
https://	**paris2024.**	**tickets.org**	**/test**

Look out!
Here, "paris2024" and "tickets" have been switched so the domain name is now tickets.org – not an official website. The presence of paris2024 in the subdomain does not mean the website is legitimate. Only the domain name can indicate whether the website is legitimate.

× **Malicious URL:** https://website.malicious.org/abc?test=paris2024.org

Protocol	*Subdomain*	*Domain name*	*Path*
https://	**website.**	**malicious.org**	**/abc?test=paris2024.org**
	The domain name here is "malicious.org"		*The presence of paris2024.org in the path does not mean the website is legitimate.*

To find out more:
ENISA – Phishing / Spear phishing

HOW CAN I PROTECT MYSELF ONLINE?

UPDATE MY DEVICES

Digital devices and the software we use every day can contain security flaws that may be exploited by cybercriminals. To address these risks, software companies and manufacturers provide updates (patches) to fix these security flaws.

Although performing updates is often seen as an annoying task, it is essential to protect yourself online.

Take care of your equipment by following best practice.

➔ UPDATE ALL YOUR DEVICES AND SOFTWARE PROMPTLY

➔ TURN ON THE OPTION TO DOWNLOAD AND INSTALL UPDATES AUTOMATICALLY

➔ DOWNLOAD UPDATES FROM OFFICIAL WEBSITES ONLY

* or app stores.

➔ MAKE REGULAR BACKUPS OF YOUR DATA AND SOFTWARE

It is recommended to check that you have a backup before running an update.

To find out more:
CISA – Understanding Patches and Software Updates