#WorkingSafeOnline Guideline

Based on Security Principles

Working in digital environments has always been challenging from a security perspective. Starting with the COVID-19 pandemic and lockdown measures, even more citizens had to depend on digital means, for both personal and professional purposes - a context in which security has become an ever-increasing concern.

With great digital benefits come equal risks, nevertheless, this should not be a cause for panic or fear of using the new technologies. On the contrary, this is the best time to change our digital habits by embracing technology with a responsible attitude.

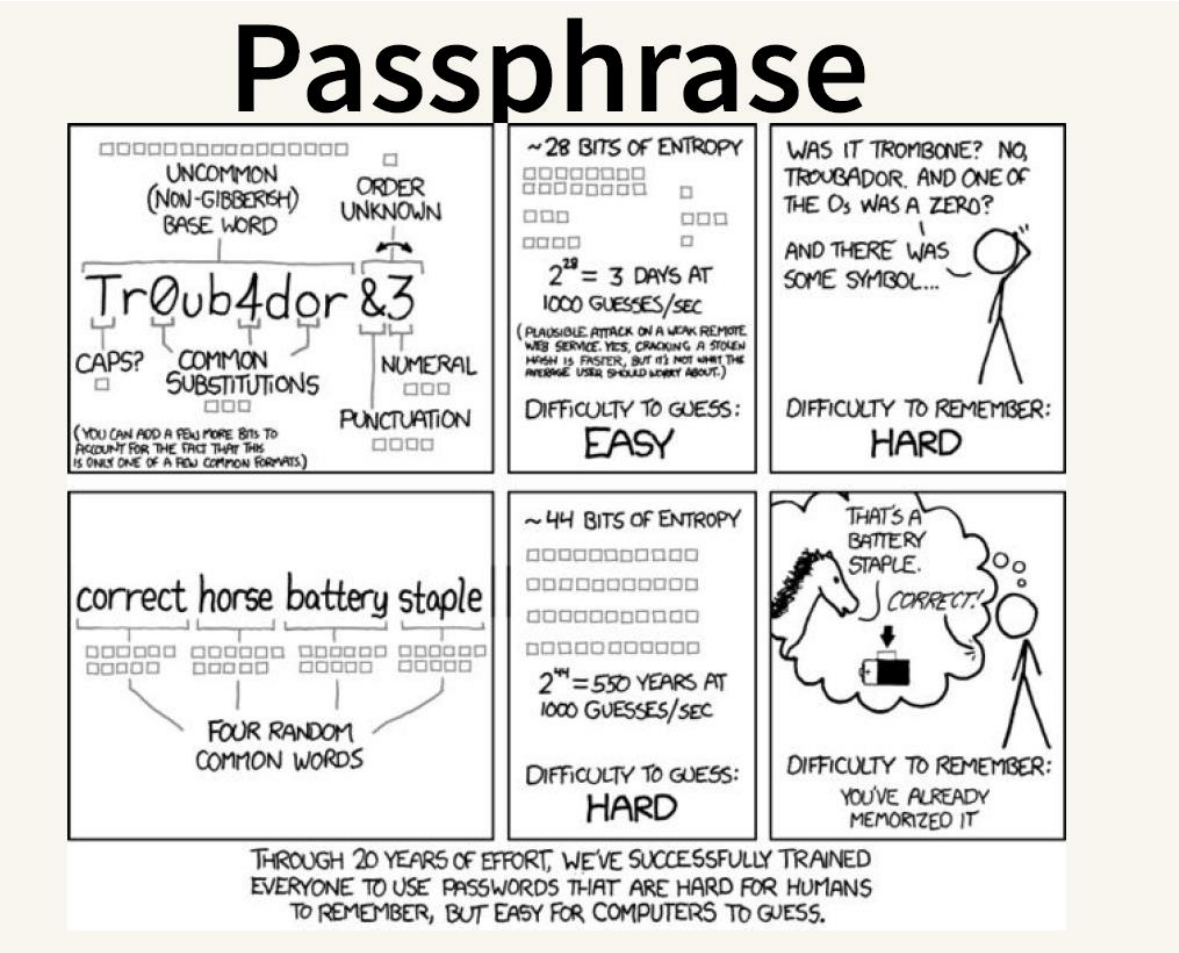
The current Guideline is dedicated to both *individuals* (teachers, students, teleworkers, parents or everyday digital citizens) and *organisations* (Civil Society Organisations, Small and Medium Enterprises, freelancers).

Our aim was to publish a series of Best Practices that could ensure minimum safety measures for everyone, explaining the basics and providing examples that could make the digital transformation more accessible to all users. The practices and examples included in this Guideline are not exhaustive, as in terms of digital security and safety there is much more happening around us.

We hope you find it useful and invite you to share with us your personal experiences in the digital world. Do not hesitate to reach out to us if you have any feedback, recommendations or new ideas at contact@digitalcitizens.net.

Long passwords / 2FA

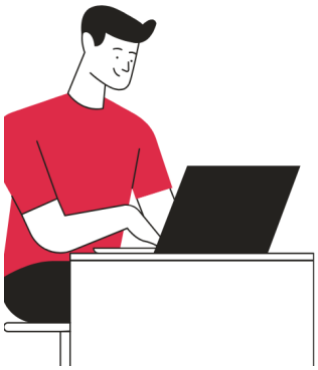
- ***Pick a long password*** made up of six or more random WORDS (Passphrase) to lock your computer or six or more numbers as a PIN to lock your phone.
- Turn on ***"two-factor" or "two-step" authentication*** on your Google, Facebook or other online accounts.
- ***Safeguarding passwords*** - Don't reuse passwords! Use a password manager if possible.



⇛ *If you are interested in finding how secure your password is, you* ***can test it here****!*

Be aware of who has access to your data and which data you share

- ***Assess the tools*** you use.
- Check your ***privacy settings*** on your social network accounts. These sites might be giving out more information about you than you intend to share.
- ***Monitor*** your accounts for suspicious activity.



⇛ *Take a look at this project if you are interested in understanding and controlling better your* ***data traces*** *https://myshadow.org/.*

Pay attention to what you click on

- Avoid clicking on suspicious links or email attachments, especially from people you don't know. Your online habits could create more risks than the malicious intentions of others.
- Avoid submitting ***sensitive information*** on websites accessed through links sent by an unknown third-party via email. If possible, it is better to manually type the website URL in your browser instead of clicking a link in order to avoid phishing.
- Only install apps from ***trusted sources***, stop downloading Pirated Applications.

⇛ *Phishing - is the fraudulent attempt to obtain sensitive information such as usernames, passwords and credit card details by disguising oneself as a trustworthy entity in an electronic communication.*

Backup your data - one of the best practices that needs to be taken into account on a daily basis.

- ***For your PC*** you can use a USB sticks, external hard disk or NAS (Network Attached Storage - usually used for more than one PC)
- ***Cloud storage*** - you can choose from a variety of providers such as - iCloud, Dropbox, Google Drive and OneDrive - to backup documents, files, photos - definitely the handiest nowadays, easy to access and to share with one condition - Internet connection. You just need to be careful with the sensitive data, especially when using free accounts.
- ***Smartphone*** - depending on the operating system, it usually saves the data in the cloud. Check the settings in order to decide what you save and how often. You can decide to backup your phone manually by downloading the content on your PC.
- ***Organisation's website*** - make sure you have a local copy of your website. Check the backup policies with your hosting provider and on the CMS (Content Management System) you use. For example, WordPress has special plugins just for Backup.

⇛ *Here you can find more information on the pros and cons of all these ideas!*

Keep Your Device Secure & Updated

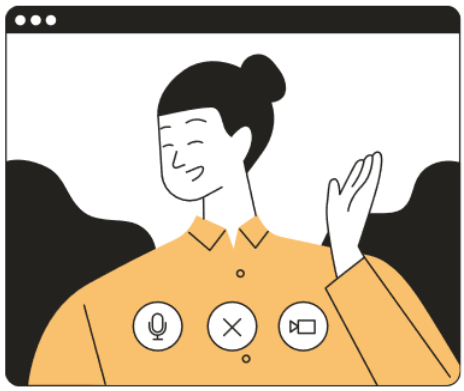
● Keep your device's ***operating system updated***, you can turn on Automatic Updates.

● Use web browsers such as Chrome or Firefox that receive frequent, automatic security updates.

● Make sure to keep ***browser plug-ins up to date*** (Flash, Java, etc.).

● ***Encrypt your data***. Most devices are capable of employing data encryption - consult your device's documentation for available options or read more on this topic.

CONNECT wisely from outside the office - from home to remote server office files or when using a public network link in a café, during your commute, at a restaurant, hotel, or elsewhere



- Don't ever use the Internet on a computer that does not have an ***antivirus*****,** antimalware, and/or firewall software installed. If you do, there is an increased possibility that a hacker can install malware or keylogger that eavesdrops on you.
- Use a ***firewall*** - Mac and Windows have basic desktop firewalls as part of their operating system that can help protect your computer from external attacks. Read more about what a firewall does!
- Use a VPN (Virtual Private Network). It works as a protected tunnel for the data. Instead of exposing data to the person who controls the network, you send it all through a trusted provider instead. If your organisation doesn't have one, you should definitely read this guideline and talk to an IT consultant.

⇛ ***Antivirus*** *definition - sometimes also called* ***anti-malware****, is a software/programme designed and developed to protect computers from malware like viruses, computer worms, spyware, botnets, rootkits, keyloggers and other similar ones.* ***Antivirus*** *programmes function to scan, detect and remove viruses from your computer. Install antivirus programmes only from a known and trusted source. Keep virus definitions, engines and software up to date to ensure your antivirus program remains effective. Here is an updated overview!*

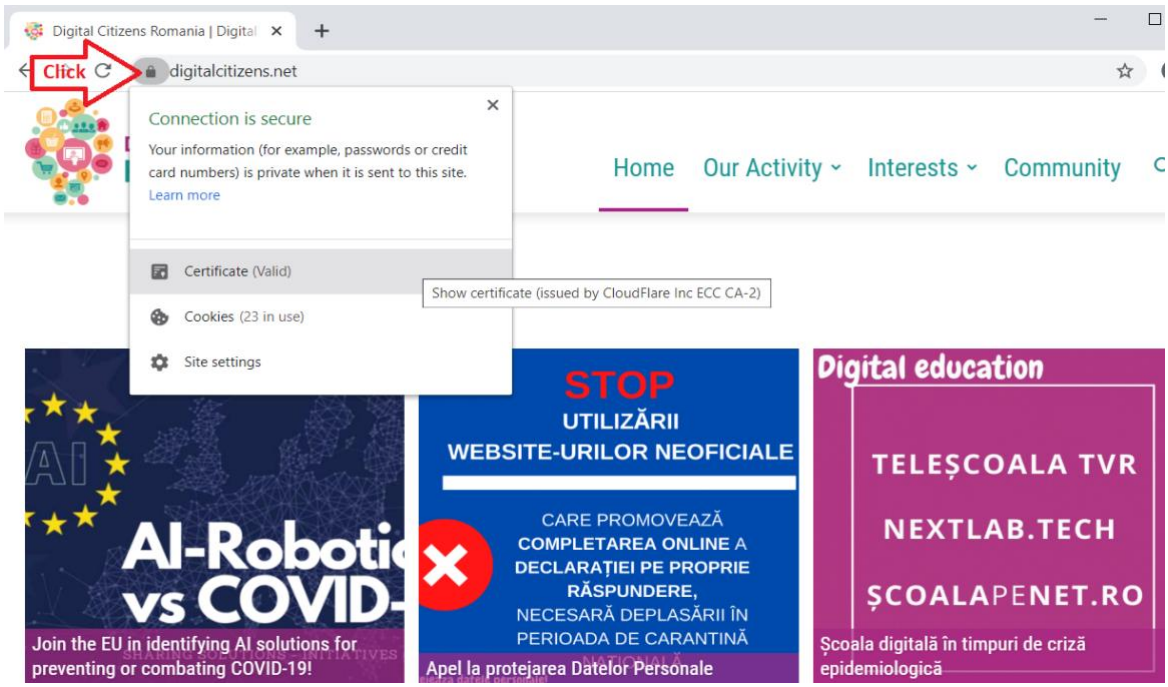
Protect sensitive data

- Be aware of sensitive data. If your organisation handles/processes data like credit card information, student records, health information and any other personal information you should particularly pay attention to the ***GDPR rules*** *(General Data Protection Regulation, enforced since 25 May 2018 to everyone who interacts with citizens in the European Union Member States).*
    - GDPR applies to all organisations - big companies but also all SMEs and NGOs, nobody is exempted!
    - Pay particular attention to the Principles of GDPR and the citizens' rights - train properly your staff and inform your beneficiaries.

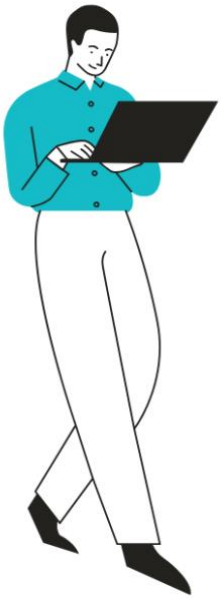
- For more practical examples you can also check the UCB Data Classification Standard, including data protection levels and associated restrictions. Be aware that the examples included in the link are not necessarily compliant with all GDPR rules.
- Assign a person in your organisation to manage this kind of data.

- Keep sensitive data off of your workstation, laptop, or mobile devices and remove this kind of files from your system when they are no longer needed.
- Access online Banking or shopping services only on trusted devices and networks and always logout of these sites when you've completed your transactions.
- Always use encryption when storing or transmitting sensitive data. With key websites that require a login, pay careful attention to make sure that there is a padlock in the browser bar HTTPS or Secure Sockets Layer (SSL) certificate, and that the URL is actually correct and not a modified version of the actual website.

Here is how to verify HTTPS/SSL Certificate on Chrome (other browsers are similar; if the connection is encrypted you will always find the padlock icon):



Know what to do if you become a victim



- If you receive warning messages about suspicious activities or if you notice activities that you don't recognise doing yourself
  - the first thing you have to do is change your password!
  - second, control other accounts connected with that profile. For example, if you log in with a Google account on your University account you should also check that.
- If you suspect an Identity theft or other kind of online attack you should report it to our national CERT and police, don't hesitate to reach out to them!
  - For Romanian citizens use the CERT.ro report form and contact the Romanian police.
- Alert the bank if you have issues with your credit card or if you have shared information about the Internet banking with suspect entities (via SMS, phone or email, on e-commerce sites, etc.)
- Report the scam/fraud directly on the platform you used to open "the offer", in case you identify false advertising (especially Facebook and other social networks)
- In the case of phishing, alert also the "victim" company (e.g. if you notice a false offer that pretends to come from a known bank or online shop, but the URL is not the original website, you should inform them about the situation as well, after alerting CERT or the Police).
- In case of loss or theft of your phone use Apple's Find my iPhone or the Android Device Manager.

Separate your private life from your professional life

- Don't use your social media private profile for your association/organisation too. It isn't ideal to have clients connecting on your private Facebook account. Instead, create a Facebook/Twitter/Instagram page for your organisation and have your beneficiaries/users connect with you over that account.
- Don't use your personal email address for work-related activities.
  - Create a separate, professional email address, strictly for the organisation work and ensure the password is different from that of your main email address.

- Ensure that you have an official account for the organisation and then separately for each member that represents the organisation.
- Ideally, you should not use Yahoo, Gmail or other generic email platforms. If you have the resources, invest in a personalized domain name.

The **Working Safe Online Guideline Based on Security Principles** is created by the Digital Citizens team:

- Mihaela TUDORACHE - research, content development, text adaptation, visuals*
- Veronica ȘTEFAN - content development, editing

Follow the Digital Citizens community via your favourite media channel

- Facebook.com/DigitalCitizensRomania/
- Linkedin.com/company/digital-citizens-romania
- Twitter.com/DigitalRomania
- Youtube.com/channel/UC_p4vd6Y9E4eivHpz8tPssg

Other useful resources

- Report tool for cybercrime online in all Europol countries
- Report (pdf) on Cybercrime and Disinformation in the time of COVID-19, Europol
- EU Agency for Cybersecurity (ENISA), Resources for COVID-19
- Resources provided by TechSoup Association to nonprofits around the world
- A free resource for digital security enthusiasts Security Education Companion

*The visuals included in the Guideline and the campaign promoting its content have been created using Canva application.