Cybersecurity for Beginners

General tips and mistakes to avoid

1. Recognize the origin of fraudulent emails, SMS and phone calls

Most of the online scams are conveyed by phone calls, emails and SMS that have all the appearance of coming from known bodies and reliable sources, often large companies, banks and even public bodies. So the first thing to do is to verify the origin of the communications, in particular those that ask for personal data, credentials, device codes or that invite you to click on a link.

- Check the address from which emails come and the phone numbers from which calls and text messages come.
- Carefully check the sender's address of the emails and the text of the links they contain: scammers often use texts that differ little from the official ones of the companies.
- The text of emails and messages can also give you an indication of their fraudulent nature, as they often contain spelling and syntax errors.
- Finally, remember that scams are sometimes complex, as fraudsters can coordinate and act on several channels (for example, by making a phone call after sending SMS).

2. Don't rush

Very often, scams rely on a sense of urgency and an invitation to act immediately. For example, the communication warns of an expiring service, a failed payment or the possibility of a current account being blocked and invites you to act quickly or even immediately.

- In any regular context, you always have time to renew a service or to intervene on a payment transaction.
- Do not act on impulse and take the time to verify, for example through a phone call to the company that provides you with the service or a check on your reserved area, the veracity of the communication.

3. Pay attention to particularly advantageous proposals or promises of money or easy earnings

Bargain price offers, oddly advantageous loans, and suspicious online trading proposals could turn out to be scams.

- Always check the goodness of the offer by comparing it to similar offers and looking for information about the provider.

4. Check the web pages on which you make your purchases

On web pages that offer purchases, it is always good to pay attention to the presence of some basic elements, such as: the "https" address, the presence of the padlock in the address bar (which indicates that the site is protected by international security systems) and the seller's data, such as the VAT number, the registered office of the company, contact details, general terms and conditions of sale, or a secure payment system that clearly states the shipping costs.

- Also remember that, on the website of the Revenue Agency, you can check the tax data reported on the web page.

5. Use the utmost caution when handling personal data, information and documents

If you are asked to communicate personal or sensitive data or to send copies of personal documents, you must be very careful: send copies of your documents only if necessary and in a reliable context and make sure of the identity of the interlocutor.

6. Keep your software and passwords up to date

In addition to periodically changing passwords, it is necessary that the operating systems and applications of PCs and smartphones are always up to date.

- In particular, check that the browser you use is up to date and periodically delete cookies and temporary files using the appropriate tools in your browser.

I fell victim to a scam, what can I do?

Being a victim of a scam is an eventuality that can happen to anyone. If, despite all the precautions put in place, you have fallen victim to a scam, it is always possible to take action to report what happened to the police. In the case of a scam that took place online, it is advisable to refer to the Postal Police who have jurisdiction over computer crimes.

- Gather all the material that can prove what happened.
- Also, if you are concerned that you have fallen victim to a bank scam, contact your bank to block your payment cards and to check that there have been no fraudulent payment instructions.

Misconceptions about cybersecurity

Myth: Clicking on the "unsubscribe" links in spam emails will stop them.

Fact: By clicking on such links, your email address may be confirmed by spammers, potentially increasing the amount of spam.

- Here are some safer ways to unsubscribe and deal with spam emails:
    - Set up filters in your email client to automatically move spam emails to the junk or spam folder.
    - Use the "Report Spam" option in your email client to train your spam filter to recognize and block similar emails.
    - Use the "unsubscribe" link only if you recognize the sender and trust the email. For other emails, it is safer to delete them without clicking on any links.

Myth: Factory reset completely erases all data from my device.

Fact: After a factory reset, you can still recover your data, unless you properly overwrite it with specialized software.

Myth: My device is safe if I never connect to the internet.

Fact: Even offline devices can be vulnerable to malware via USB drives or other physical connections.

Myth: Closing the lid of your laptop is the same as disconnecting.

Fact: Closing the lid only suspends the system. It doesn't log you out, leaving your session vulnerable to unauthorized access. It is recommended that you log out of your computer.

Myth: Airplane mode is enough to protect your device during the flight.

Fact: Although airplane mode turns off wireless signals, it does not protect against pre-installed malware or unauthorized access if you physically access your device.

Protecting your social media security and privacy

Recommendations:

- **Use strong and unique passwords:** Create strong and different passwords for each account. Use a password manager to store them securely.
- **Enable two-factor authentication (2FA):** Add an extra layer of security by requiring a second verification factor in addition to your password.
- **Check your privacy settings:** Review and update your privacy settings regularly to limit who can see your information and posts.
- **Be wary of suspicious links:** Don't click on links that are suspicious or from untrustworthy sources, as they may be phishing attempts.
- **Limit the personal information shared:** Avoid sharing sensitive details such as address, phone number, or financial information.
- **Use secure Wi-Fi networks:** Avoid connecting to unsecured public Wi-Fi networks to access your social accounts.
- **Check app permissions:** Control what permissions you grant to social media apps and limit access to unnecessary data.
- **Monitor for suspicious activity:** Keep an eye out for unusual activity on your accounts and report any issues immediately.
- **Educate yourself and others:** Educate yourself on safety best practices and share this information with friends and family.

Mistakes to Avoid:

- **Use the same password for multiple accounts:** If one account is compromised, everyone else with the same password is at risk.
- **Ignore security updates:** Not regularly updating apps and devices can leave exploitable vulnerabilities.
- **Accepting friend requests from strangers**: These could be fake profiles created to collect personal information.
- **Share your location in real-time:** Avoid sharing your current location, especially in public posts.
- **Don't log out of shared devices:** Leaving your account open on shared devices can allow others to access your information.
- **Don't monitor for suspicious activity:** Ignoring signs of unusual activity on your accounts can lead to security issues.
- **Sharing too much personal information:** Posting sensitive details can facilitate identity theft.
- **Not educating yourself on security practices:** A lack of knowledge can leave you vulnerable to attacks.

Quiz

1. How can I verify the origin of a suspicious email?

a) By clicking directly on the links in the email.

b) Carefully checking the sender's address and the text of the links.

c) By immediately replying to the email to ask for confirmation.

d) Forwarding the email to all contacts to notify them.

2. What is a warning sign in fraudulent communications?

a) The presence of particularly advantageous offers.

b) The absence of spelling and syntax errors.

c) The request to act calmly and without haste.

d) The origin of a known telephone number.

3. What to do in the face of a suspicious online trading proposal?

a) Invest immediately so as not to miss the opportunity.

b) Check the goodness of the offer by comparing it with other similar ones.

c) Provide your financial details to receive more information.

d) Share the offer on social media to get opinions.

4. What elements indicate the reliability of a shopping web page?

a) The presence of offers at bargain prices.

b) The "https" address and the padlock in the address bar.

c) The absence of seller data.

d) The request for payment by bank transfer.

5. How to manage the request to communicate personal or sensitive data?

a) Submit all required documents immediately.

b) Send documents only if necessary and in a reliable context.

c) Share data on social media for added security.

d) Ignore the request to avoid risks.

6. Why is it important to keep software and passwords up to date?

a) To receive personalized advertising notifications.

b) To protect against vulnerabilities and security risks.

c) To speed up internet browsing.

d) To increase the storage space of the device.

7. What to do in case of an online scam?

a) Send a protest email to the scammer.

b) Contact the Postal Police and collect all evidentiary material.

c) Delete all your online accounts.

d) Share the incident on social media to alert other users.

8. Which of the following is a good practice for online safety?

a) Use the same password for all accounts.

b) Clicking on suspicious links out of curiosity.

c) Enable two-factor authentication (2FA).

d) Share your real-time location on social media.

9. What common mistake increases the risk of being a victim of scams?

a) Update your apps and devices regularly.

b) Check app permissions.

c) Use unsecured public Wi-Fi networks.

d) Use strong and unique passwords.

10. What is meant by Phishing?

a) A technique to improve the internet connection.

b) An attempt to obtain sensitive information via suspicious links.

c) A method of automatically updating software.

d) A secure online payment system.

Solutions:

1. b
2. at
3. b
4. b
5. b
6. b
7. b
8. c
9. c
10. b