Lamberti

Smart Digital Habits

Our security depends on you

July 2021

Every day we take precautions to keep safe.

We leave the house early if there is traffic, take an umbrella if thunderstorms are forecast, use potholders to drain pasta. We do not give our house keys to a stranger who stops us on the street and when we notice strange behavior we become alarmed. Safety is a priority in private life as well as at work: we use hard hats, we walk on walkways, we don't walk down stairs looking at our cell phones.

In our daily lives, we are mindful of our own "safety" and that of our loved ones. But safety must be an important part of our digital lives as well: at home and at work we need to be aware of dangers. Following some good habits helps us protect ourselves and protect our company. Cyber risk is growing and we must all be more careful.

Keep an eye on your Passwords!

The password you use at work should be unique and should not be similar to the ones you use in your private life.

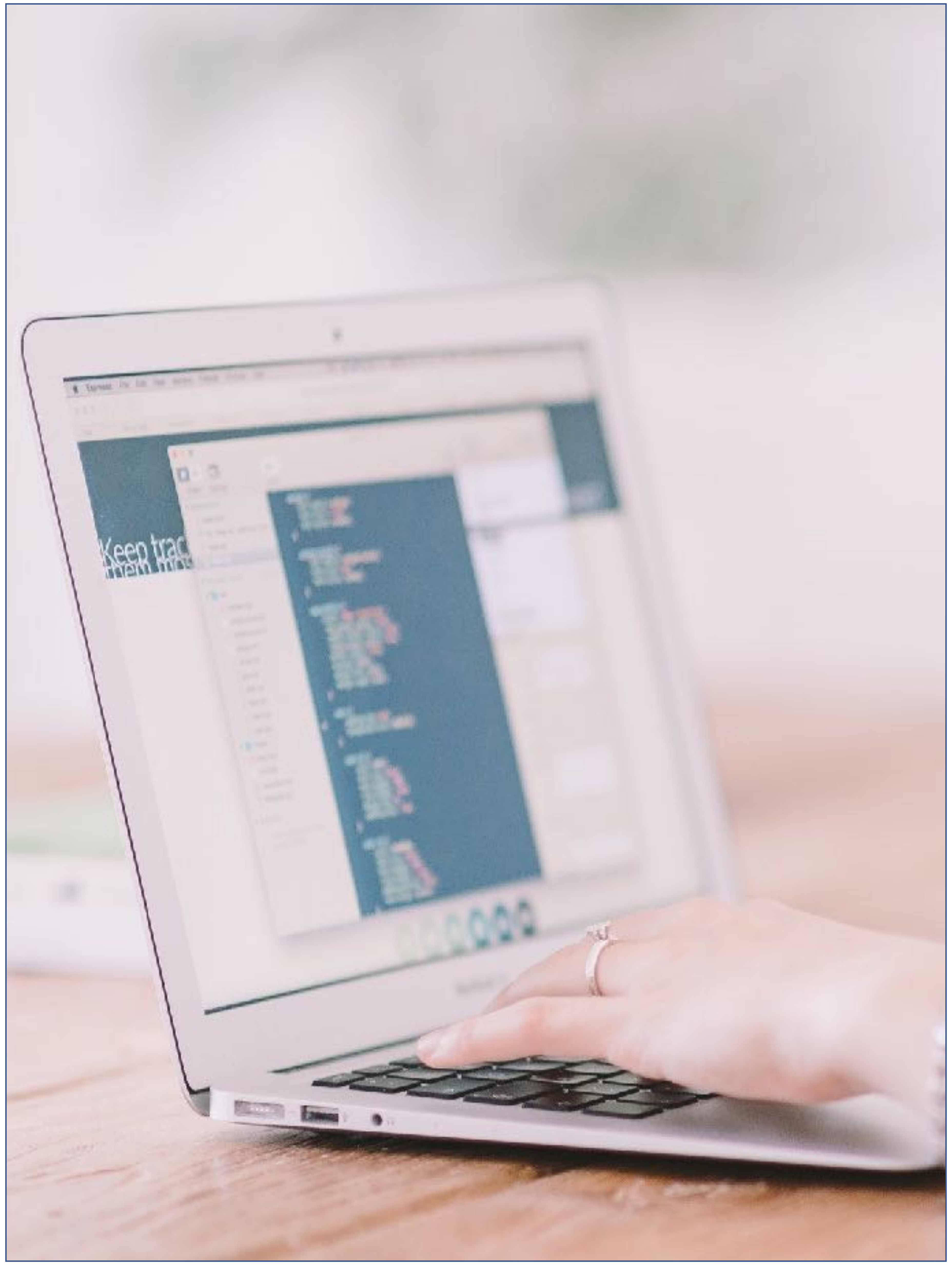
If in doubt, use a phrase that is important to you or easy to remember, such as “mymotherhasredhair". Change your passwords frequently and completely (don't add numbers to your existing ones but use different ones).

Use different passwords to access the corporate network, SAP, Zucchetti, etc. This way if one password is compromised the others remain safe. Don't share your passwords with others.

E-mail...

... is not as safe as we think. Do not use it to send sensitive information such as passwords, banking information, credit card information, personal requests, etc.

Use corporate email for business communications only. If you have to send files that contain confidential information, always protect them with a password and communicate it to the recipient with a different tool than email (for eg. by text message or WhatsApp). Do not respond to any message that asks you to access external web pages and enter your log in information. Do not respond to any message that seems suspicious or fraudulent and report it immediately to our IT services ictsecurity@lamberti.com. Do not respond to messages from generic addresses such as info@.... or sales@....



Who is writing?

Don't stop at the sender's name you see on the email message.

Check it by clicking on it to verify the full address. Delete all emails with domains you do not recognize. Be careful, hackers can enter authentic email exchanges.

Read the text carefully

Are there any grammatical errors in the text of an email or text message? Strange phrases? Abnormal syntax?

These could be useful clues to identify a fraudulent email message.

Do not act and contact our IT services **ictsecurity@lamberti.com**

New or urgent instructions? Stop!

Have you received an email from a customer, from a contact at the company, even if a senior one, from a supplier with new banking instructions, a request for an urgent funds transfer, changes to the usual Lamberti Group purchasing and selling procedures?

Never follow up on these requests. Contact our Company's Administration or Finance Department by phone (not by email) and ask them to verify the authenticity of the communication.

Do not click on links

Have you received an email, WhatsApp or text message asking you to donate funds? A chain letter? A notification of a prize you won? An invitation to enter a contest? Don't click on the links or forward the email to friends or colleagues.

Scams, traps and computer hackers often hide behind a link. Notify our IT services at **ictsecurity@lamberti.com** immediately, even if you clicked on it by mistake. If you do so promptly, you can prevent a cyber attack.

USB flash drives?
No Thank you :-)

Where did the flash drive come from? Who used it last? Was it given to you as a gift? Did you find it?

Flash drives can spread "malware," small software programs that spread quickly and can endanger the corporate network. Do not use them on company computers.

Phone, text, WhatsApp frauds

Cybercriminals are very sophisticated. Watch out for text and WhatsApp messages you receive with links as well as phone calls with requests for information.

Do not disclose passwords or private information without verifying the real identity of the interlocutor, even when it seems to be a colleague or a service provider (electricity supplier, gas, telephony, bank, insurance company, ...).

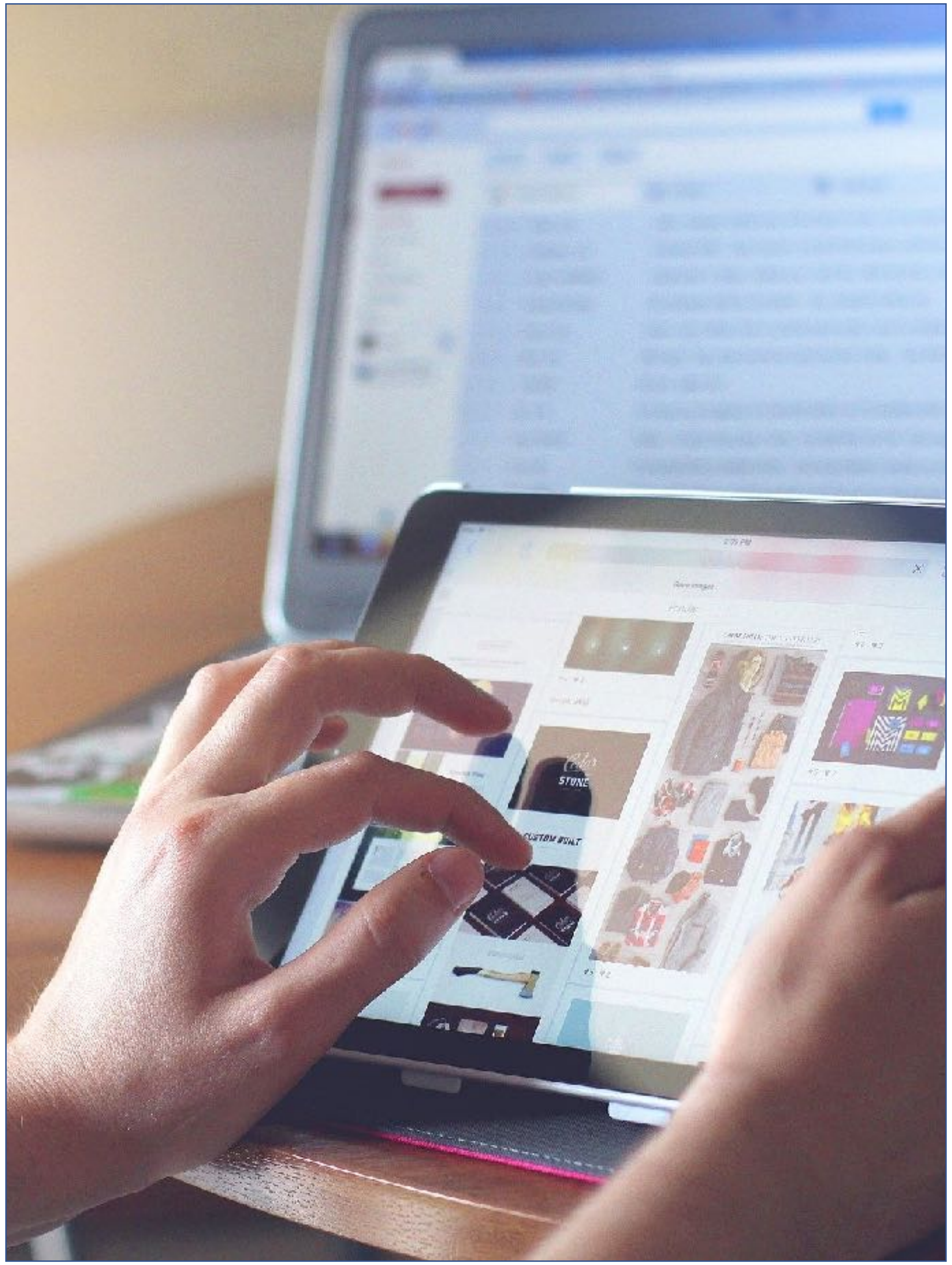
If you receive a text message from a number you don't know, google it and verify if there are comments from other users.

Watch out when you surf the net

Don't stop at the padlock next to the address, click on it and make sure the name matches the address; possibly rewrite the address avoiding links that don't show where they take you.

Always pay attention to sites and online navigation. All it takes is a lack of caution, a wrong click, a page left open. Always check the address, don't get carried away by haste or curiosity.

If something seems odd, report it **ictsecurity@lamberti.com**, it could be a sign of an intrusion attempt.



Authentic site or scam?

There are clone and scam sites that look authentic.

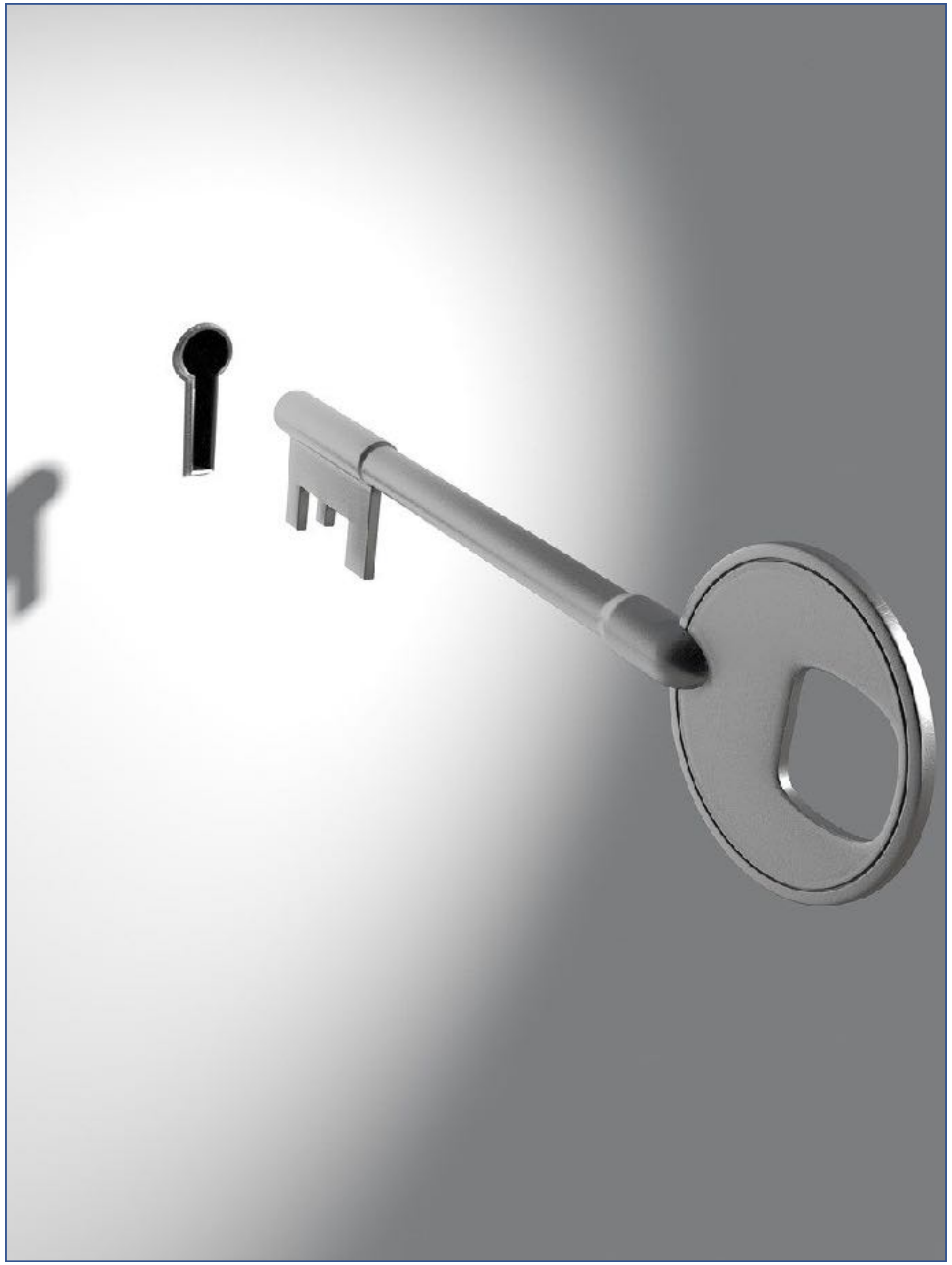
Here are some elements that help you identify a possible clone/ scam site: **lack of indication of the seller's data** (head office, telephone, VAT number, company registration number, etc.), **grammatical or spelling mistakes in the text of the site, lack of privacy policy or general conditions of sale, unusual payment methods** (eg. acceptance of bank transfers only), **use of a name for the site that does not relate to the activity carried out** (eg. a name related to food for a site that sells shoes), **sale of branded products** (especially in the clothing sector) **at extremely advantageous/out-of-market prices**. These are simple clues, but they should put you on alert.

Your privacy is a valuable asset!

Always check your settings to know what data you are making public. If you do not know how, ask for help.

For example, on your smartphone make sure that geolocation data is only active when you use specific applications. On social networks, don't geo-locate your photos, don't make public your travel or vacation periods, don't accept as a friend or confide in people you don't know, don't provide personal information, don't indicate where you live or where you work.

Be careful about the images you post online.



Lamberti

Smart digital habits protect all of us and our company.

Lamberti