SHIRUDO
A CYBERSECURITY SERIOUS GAME

CHECK LIST PHISHING

#Mission 10

One negative answer to one of the points should make you vigilant. 2 (or more) negative answers should alert you.

In that case, do not open the attachments and do not click on any link in the email.

Before opening the email:

- ☐ **Source:** Do I know this sender?
- ☐ **Address:** Is the sender's email address the one customarily used?
- ☐ **Subject:** Does the subject correspond to the nature of our customary relations?

Content of the email:

- ☐ **Contact person:** Am I the most appropriate contact person?
- ☐ **Signature:** Is the signature identical to the previous ones?
- ☐ **Content:** Does the email contain any spelling mistake or grammatical error?

Your intuition!

- ☐ **Nature:** Does the intent of the email correspond to our customary relationship?
- ☐ **Emotion:** Do I have any feeling of fear, eagerness or exuberance on reading the email?
- ☐ **Sixth sense!** Can I assert that I have no doubt on reading this email?

Emotion is our worst enemy in this situation The wrong "click" could put your organization in an irreversible situation.

Any doubt? Never take any risk, contact your IT support!

PRACTICAL EXAMPLES TO ILLUSTRATE THESE CHECK POINTS

First checking reflexes: Source / Address / Subject :

These three items of information can be checked **BEFORE** opening the email

- **Source**: Do I know this sender?
- **Yes**, it's clearly from your bank.

An email coming from another bank would already be suspicious.

- **Address**: Does the sender's email address seem correct?
- **Yes**, it's clearly the usual email address.

An address such as "noreply@l-mb.com" would be the sign of an email to be deleted because of the dash inserted in the domain name.

The domain name is the name positioned after the @ in the email address, in this case **lmb.com**.

This name is generally the same as the name of the website. To check it, do a search for the organization (in this case the LMB bank) via an internet search engine. Then compare the address proposed by the search engine with the domain name of the email: they should be identical.

- **Subject**: Does the subject correspond to the nature of our customary relations?
- **Yes**, you have just obtained a new account, and at first sight the subject is in line with your customary relations.

However, you had already received an email confirming the activation of your account by the bank, so this second email is a first sign, which should alert you and lead you to delete the email or contact the bank.

A subject such as "Confirmation of your IDs" would definitely be inappropriate coming from a trusted institution such as a bank.

Level 2: Contact person / Signature / Content

This is the general appearance of the email

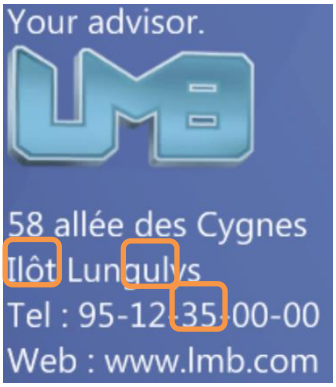
- **Contact Person:** Am I the most appropriate contact person?
- **Yes**, undoubtedly, you have a personal account at this bank. It is legitimate for the bank to contact you.

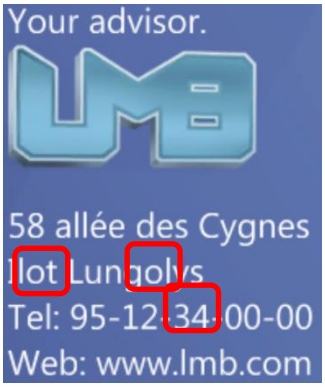
The email address of your account corresponds to your address.

The email address of your account corresponds to your address. An address such as "Cl@alterys-city.com" would be suspicious, because the name of the city is spelt incorrectly.

- **Signature**: Is the signature identical to that in the previous emails coming from the same sender?
- **No**, in this case you note errors which should definitely lead you to delete this email.

Comparing it with the first email received from the bank, we can note the three differences shown in the boxes below:





- **Content** (spelling and grammar): Is the email free of spelling mistakes and grammatical errors?
- **Yes**, no mistake can be noted in this email.

Coming from an institution such as a bank, an email with mistakes would be a sufficient criterion to delete the email.

Analysis of the "clickable" link in this email remains a very complex operation, and it is preferable to use specialists.

In this case, however, note that the presence of the "Https" and the correct domain name "lmb.com" are factors inspiring trust. Wrongly so, of course!

Level 3: Your intuition - Nature / Emotion / Sixth sense

Be vigilant, and pay attention to your feelings…

- **Nature**: Is the intent of the email questionable?
- **No**, the intent is to worry you by suggesting that information is missing and that your account might not function, to force you to confirm information already possessed by the bank, and click on a link.

With good intent, the bank would have sent you an email stating that to its knowledge your email is "Cl@alterrys-city.com", and that if you note an error, you should contact them.

- **Emotion**: Can I assert that I have no feelings of fear, eagerness or enthusiasm on reading this email?
- **No**, as the intent is to make you think that information is missing and that your account might not function, it is trying to persuade you to confirm information already possessed by the bank, and click on a link.

You will often find emails proposing promotional offers, links to view photos of an event, arousing fear of seeing your account closed or deleted, or asking for charity, etc.

- **Sixth sense:** Can I assert that I no longer have any doubt on reading this email?
- **No**, several clues show that this email is probably dangerous.

If you have answered Yes until now, but you hesitate on this last question, which is admittedly the most subjective one, **take no risk**, call on a specialist or call the sender of the email, without using the phone number in the suspicious email, which could route you directly to the counterfeiters!

Conclusion

Analysis and verification of the links present in an email **are not sufficient** to determine with any certainty the presence of a phishing email.

You should take the time to check the 3 points listed in Issue 1 BEFORE opening the email, and check the email's general appearance.