PHISHX

TIPS TO AVOID *PHISHING AND MALWARE*

Be wary of great deals

As tempting as that super cheap trip, that unmissable promotion or that e-mail full of questions that promises to remove all doubts with a simple "click here", be suspicious! That is where the pitfalls hide, which put you and your co-worker at risk.

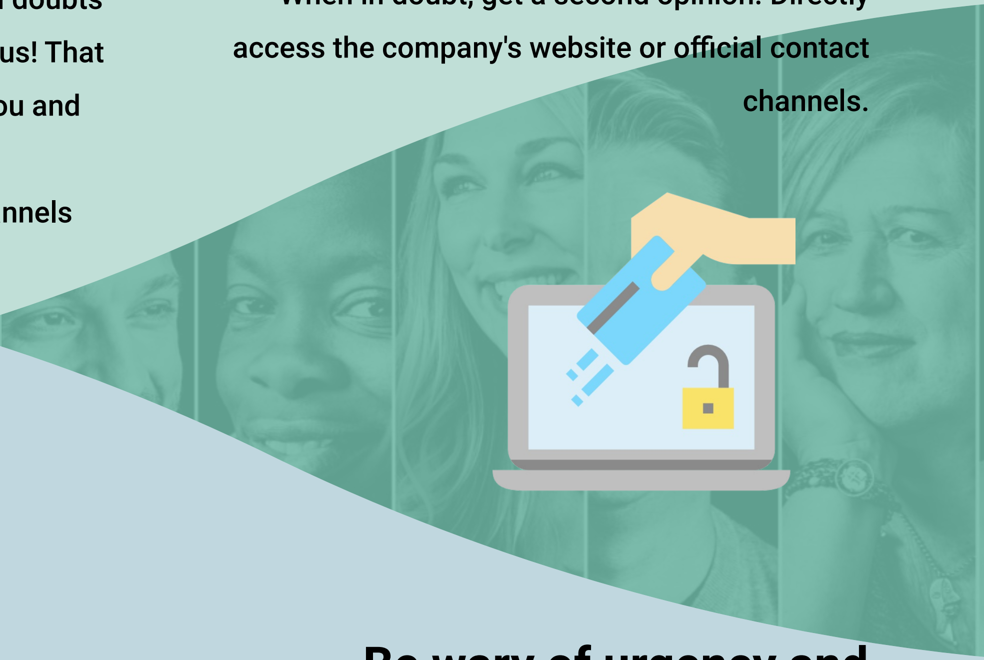
Remember the company's official channels for disclosing benefits to users.

Be wary of suspicious messages

The name and sender address that appear in the message can be easily changed to show false information.

Legitimate companies and banks do not send messages without proper registration and consent, under no circumstances. Therefore, do not believe in messages from sources that you have not previously registered and approved.

When in doubt, get a second opinion. Directly access the company's website or official contact channels.



Be wary of urgency and deadlines

Provoking a sense of urgency or fear is a common tactic. Watch out for messages that appeal too much for your attention and that, in some way, threaten you if you do not follow the described procedures.

Watch for messages, received on behalf of an institution, that try to trick you into supplying information, installing / running programs, or clicking on links.

phishx.io

PHISHX

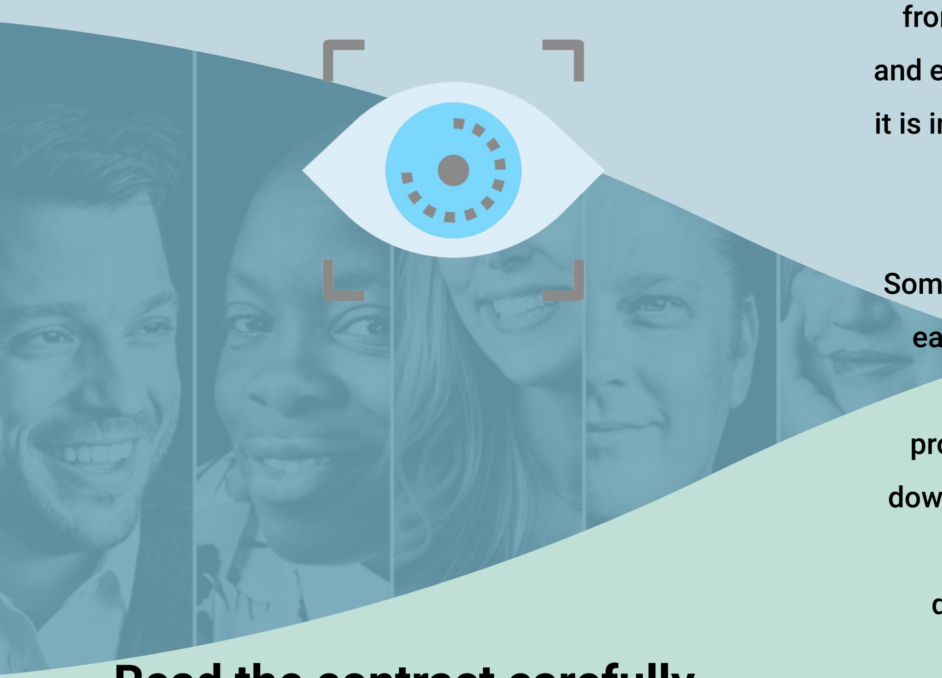
TIPS TO AVOID *PHISHING AND MALWARE*

Care with links and attachments

When receiving a questionable message, do not access links or execute the attached files.

Check the link shown in the message. Scammers often use techniques to obscure the actual link to Phishing. By placing the mouse over the link, it is often possible to see the real address of the fake page or malicious code.

If the link address looks strange, do not click on it!



Read the contract carefully

It seems like a boring thing to do - and it really is. However, it is necessary. Some contracts or terms, which we accept without reading, authorize our information saved on the machine to be sent to third parties to have access.

And then we know what can happen: invasion.

Do not run unnecessary files

If you received a box of chocolates in the mail from an unknown person, would you open it and eat it all without hesitation? No. Likewise, it is important to be careful when an unknown person sends a suspicious email having attachments and images.

Some websites and applications allow you to easily share files with other users. Many of these sites and applications offer little protection against malware. If you share or download files using these sharing methods, be aware of malware. The malware can disguise itself as a popular movie, album, game, or program.

phishx.io