HOW TO AVOID SCAMS AND FRAUD

The upsurge in attempts to defraud people by e-mail or by telephone calls is forcing everyone to be more vigilant.

Here are some best practices for protecting yourself against these attacks.

.

Within this general framework of vigilance, no ORCOM representative may be asked to contact you (by telephone, e-mail, etc.) to ask you to change our payment details or make a transfer not justified by an invoice.

If in doubt, you should contact your usual ORCOM contact to confirm your request.

HOW TO PROTECT YOURSELF AGAINST TRANSFER FRAUD OR FALSE BANKING INFORMATION

CONTACT YOUR CREDITOR DIRECTLY WHEN YOU RECEIVE A MESSAGE REQUESTING A PAYMENT TO A NEW BANK ACCOUNT

If you receive a message asking you to settle an outstanding payment by transferring funds to a bank account that you have never used, call your creditor on their usual number to confirm the message and the bank account details received.

BE WARY OF MESSAGES URGING YOU TO DISCLOSE YOUR E-MAIL PASSWORD

Make sure they don't take you to a fraudulent site to steal it.

APPLY SECURITY UPDATES (PASSWORDS, ANTIVIRUS, ETC.) REGULARLY AND SYSTEMATICALLY SECURITY UPDATES (PASSWORDS, ANTIVIRUS, ETC.)

To the system, applications and software installed on your devices.

INSTALL YOUR APPLICATIONS OR SOFTWARE ONLY FROM OFFICIAL WEBSITES OR STORES

By going to a fraudulent site, you run the risk of downloading a version infected with a virus.

HOW TO PROTECT YOURSELF AGAINST PHISHING?

NEVER COMMUNICATE SENSITIVE INFORMATION BY E-MAIL OR TELEPHONE

No serious administration or commercial company will ask you for your banking details or your passwords by e-mail or telephone.

BEFORE CLICKING ON A DUBIOUS LINK, POSITION YOUR MOUSE CURSOR ON THIS LINK (WITHOUT CLICKING)...

…this action will display the actual address of the link. This allows you to check the link's plausibility. For greater security, you can also go directly to the site of the organisation in question via a link that you have typed yourself.

CHECK THE WEBSITE ADDRESS DISPLAYED IN YOUR BROWSER

If it does not correspond exactly to the site in question, it is almost certainly a fraudulent site. Sometimes, just one character in the website address can change to deceive you. If in doubt, do not provide any information and close the corresponding page immediately.

IF POSSIBLE, CONTACT THE ORGANISATION CONCERNED DIRECTLY

In order to confirm the message or call you have received.

USE DIFFERENT, COMPLEX PASSWORDS FOR EACH SITE AND APPLICATION SITE AND APPLICATION

To prevent the theft of one of your passwords from compromising all your personal accounts, you can also use KeePass-type digital safes to store your various passwords securely.

IF THE WEBSITE ALLOWS IT, ACTIVATE THE DOUBLE AUTHENTICATION TO SECURE YOUR ACCESS.