PHISHING TIPS

Allianz is currently facing an increased number of fraud attempts via fake certificates, letters and messages.

Please find below some tips on how to detect phishing messages and react correctly?

What is phishing?

Phishing emails are messages that are designed to have recipients share personal information or install a malware on the computer without realizing. Most Phishing attempts are very realistic and make an effort to look official, as if they were from a bank, a payment site, an online store or they strive to impersonate known contacts.

They can have different themes, such as email account password reset, shared document, news on a current topic, invoice or payment notification, deliver a package, signing on a website or social media notification.

Even just the opening of a phishing email provides the information to the attacker, or informs the attacker, that there is someone behind this email account that is likely to click on links. **Therefore, we should avoid clicking on anything in the message until we determine whether it is real or fake**.

Tips to identify phishing emails:

Keep your emotions in check - phishing scams rely on emotional triggers like curiosity, urgency, fear, and reward to drive you to action. Look out for emotional triggers like surprising headlines referencing a current event, exciting offer, a reward, thank you emails, or unexpected bank notices.

Look for warning signs - listen to your ‘gut feeling’. Does anything in the email seem strange? Was the email sent by an unknown sender? Was it expected or unsolicited? Are there grammar or spelling errors? Does it ask for personal information? If you've answered “yes” to any of these questions, you may have received a phishing email.

Examine the domain name - some attackers modify domains to catch targets off guard. For example, if the correct domain was allianz.com, the phishers may register “alliaanz.com” or “allianz.co”, hoping you won’t notice the subtle difference.

Always verify the sender - make sure you recognize the sender’s name and domain. To check, pass the mouse over the e-mail address – most organizations will send messages from a granted e-mail address. If you recognize the sender, verify the message is legitimate with a quick phone call/chat message.

Do not click any link - hover the mouse over links to check them – usually a link shall have a page hosted on a domain part of the URL that the message refers to.

Check for spelling - make sure that the language used is correct, in common cases, attackers use unprofessional grammar, wrong terms or improper capitalization. However, they are improving in this area.

Check salutation - phishing e-mails often use a generic salutation (e.g. Dear user) instead of a personal greeting.

Never give your personal information – Allianz will **NEVER** ask for your password or PIN.

Do not fall prey to urgency - some phishing emails can sometimes require immediate action. Therefore analyse the situation before acting.

Check email signature - most legitimate senders will have a full signature at the end of their e-mails

Be careful with attachments - attackers can trick us with attractive attachments and fake brand icons, fraudulent documents/certificates.
Consider a document potentially suspicious if:

- The document contains unrealistic promises or unusual offers e.g. payment of very high sums.
- You are asked to pay a certain amount before receiving something back.
- The text is poorly written and/or contains spelling mistakes.
- Letterhead, stamp, signature and other brand symbols are not correct.

Check if the message is too good to be true - something just does not look right.

When in doubt, report the message to an Allianz Partners office - better safe than sorry, no matter the concern, check before you act!

How to protect yourself in a nutshell?

- Delete all emails with unknown or strange looking sender addresses without any checks and previews.
- Check every incoming email against the 3 explained phishing principles - if you notice anything suspicious, do not open any attachments (even Word, Excel, Power Point or pdf files can contain malware), do not click any link contained in the email (visible link text and real links may differ) if the link seems to be a well-known webpage, open the browser and type the link manually.