Protect yourself please

How do I recognize phishing emails?

Phishing is defined as the fraudulent attempt to obtain sensitive information such as usernames, passwords and credit card details by disguising oneself as a trustworthy entity in an electronic communication (source here). In our case this means that someone will try to present himself/herself as a member of Cloud68.co team and ask for your sensitive information. One of the ways to understand easily that someone is sending you a phishing email is that we at Cloud68.co will NEVER ask you for your password in an email. If you don’t trust a link in an email sent from us, go directly to our contact us page and inform us about the suspicious activity, or even better schedule a call with our team: schedule a call.

What is two faction authentication?

2FA is an extra layer of security used to make sure that people trying to gain access to an online account are who they say they are. First, a user will enter their username and a password. Then, instead of immediately gaining access, they will be required to provide another piece of information.
This second factor could come from one of the following categories:

- Something you know: This could be a personal identification number (PIN), a password, answers to “secret questions” or a specific keystroke pattern;
- Something you have: Typically, a user would have something in their possession, like a credit card, a smartphone, or a small hardware token;
- Something you are: This category is a little more advanced, and might include biometric pattern of a fingerprint, an iris scan, or a voice print;

There are various types of 2FA:

- Hardware Tokens
- SMS Text-Message and Voice-based 2FA

- Software Tokens (this being the most popular form)
- Push Notification for 2FA
- Other Forms (Biometric 2FA)

You can read more on 2FA here: What is 2fa?

Revision #2

Created 26 April 2021 13:17:33 by Redon Skikuli

Updated 7 October 2021 12:37:08 by Sidorela Uku