How to Recognise a Phishing Scam?

The Association of Serbian Banks is informing all bank clients that the trend of sending phishing messages with malicious content continues, and invites all citizens to be informed about current threats and risks, as well as to practice increased caution when opening and viewing e-mails.

Phishing scams are one of the most common forms of cyber-attacks, both due to easy distribution and difficult detection by the end user. Phishing scams use various social engineering techniques to deceive the recipient of a message by sending a purpose-made text and tricking the recipient into revealing confidential information or performing an activity (in this case, opening an infected attachment enclosed in the message).

The most recent contingent of such messages was allegedly sent from the e-mail addresses of various banks operating in the Republic of Serbia, and they contained information about the alleged foreign exchange inflow to the user's account. Please note that the addresses from which such e-mails were distributed were NOT the addresses of these banks' servers, as was stated in the e-mail, which can be determined through additional analysis by message recipients (see Instructions for Identifying the Sender of a Message on the website of the Association of Serbian Banks). This is just one of the types of attacks used by hackers, and some other common examples include using fake invoice statements, invoice deliveries, notifications on the arrival of a DHL shipment, etc. All these e-mails are characterised by the fact that they are not sent from the e-mail domain located in the sender field, as well as that they contain information which is usually not related to the recipient of the message.

If you receive one of these e-mails, or something similar that raises your doubts about its authenticity, be sure to perform an additional check of the context of the information contained in the e-mail. Do not open attachments if you doubt the validity of the message, and delete them immediately. If you open attachments, it is always advisable to perform a preventive scan with an antivirus software, provided, of course, that it has been properly updated and contains information about the latest threats.

Always follow the advice and instructions distributed by your bank, as well as the best practices and tips for safe digital business. More information on information security can be found on the following sites:

https://www.ubs-asb.com/en

https://www.cert.rs/en