Phishing refers to Internet scams in the form of fake e-mail messages that appear to be sent by legitimate organizations (for example, a bank, public authority, or online shopping site) and trick the recipient into sharing personal, financial, or security information. In this way, fraudsters gain access to usernames, passwords or credit card information. In such emails, you are most often asked to download an attached document or click on a link.

Given the frequency of online fraud, which is often successful for the attacker, citizens are reminded to be careful when sending personal information via e-mail or social networks.

Do not enter your personal information, credit card information, do not send copies of ID cards, card PINs, CVC codes from cards (the last three digits on the back of the card), as well as codes generated by mobile banking. Institutions such as banks and public authorities will not ask you to submit personal data via e-mail. Also, keep in mind that only the IBAN/account number and the name and surname of the account owner are required for payment to the account, not the data from your card (card number, expiration date and CVC code)!

Below we present the most common examples of phishing scams, how to recognize them and how to act if you receive a phishing e-mail. However, the pattern of such messages is mostly the same: the attackers use a similar e-mail address domain as the organization they represent, they call for an urgent/quick reaction, the messages often contain grammatical and spelling errors and they ask you for certain personal information, and the most common is entering data from your card. Therefore, if you do not want to be a victim of fraud, check whether the sender's e-mail address matches the official e-mail address of the institution, do not open links and attachments from suspicious senders, and do not enter or send your personal data (including card data)!

If you become a victim of fraud, immediately notify the Ministry of the Interior of the Republic of Croatia!

EXAMPLE 1. FAKE EMAILS FROM THE BANK

You are a user of x bank and as their client you receive news from the bank, information about their products or services to your e-mail address. One day you received an e-mail from the bank asking you to click on a link and thus:

confirm your bank account information;

you update the mobile banking application;

confirm a recent transaction;

confirm your identity in order to access your account again after unauthorized access by a third party (your account has been

blocked because there is a suspicion that someone has used your card unauthorized)

These are just a few examples of phishing scams that fraudsters use on banks to get financial benefits and your personal information.

How to recognize fraud?

Although the name of the bank is written under the sender and you did not suspect it at first, check the e-mail address of the sender. If it does not match the official e-mail address (domain) of your bank, delete the e-mail immediately. For example, you are a client of xbanka, which has the official domain @xbanka.hr, and you received an email from a sender whose domain reads, for example: @x-banka.com, @xbanka.eu, @hr-xbanka.com, @m-xbanka .com, it's a scam.

Check the subject (subject) of the e-mail message because the subject often states IMPORTANT, URGENT. Attackers emphasize urgency or importance in the subject line of the e-mail message in order to prompt you to react.

Check the content and correct spelling and grammar of the e-mail. Such messages often start with a generic greeting (e.g. dear customer, dear client, respected client, etc.), contain grammatical and spelling errors, and the content of the e-mail always calls for an urgent (quick) reaction (e.g. click to avoid losing your account , confirm within 24 hours and similar).

If you received a link or button that you have to click to verify your identity or update the application, it is very likely a scam. If you are not sure, you can always contact the bank, but don't click!

Check the link in the email to see where the link goes and if it matches the official domain by hovering over the link, but don't click. Remember, attackers often use addresses that are similar to official bank addresses (eg x-banka.com, hr-xbanka.com, etc.), so study the address carefully.

The attachment sent by the attackers is a malicious program, and by downloading such an attachment, sensitive, personal, financial and similar data are usually collected. Therefore, do not download them if you are not sure of the sender!

If you receive a suspicious e-mail, follow the steps listed and do not click on links, download attachments or respond to such messages. Report to the bank and delete the email!

Remember, the bank will not send you an e-mail containing a link to confirm your bank account information, it will not ask you for card information, PINs, passwords, m-token codes, and ask you to confirm via e-mail or link recently completed transaction.

The bank will not ask you to submit personal data by e-mail, but will ask you to come to the branch in person.

Example of a phishing email (e.g. you are an xbanka client whose official domain is @xbanka.hr):

EXAMPLE 2. FAKE EMAILS FROM PUBLIC AUTHORITIES

Nowadays, attackers are increasingly presented as public authorities, such as:

e-mail from the Tax Administration in which you are informed that you have been granted a tax refund, and in order for it to be paid to you, you need to click on the link or scan the QR code

e-mail from the Tax Administration in which you are requested to pay tax, and in order to pay it you need to click the link or scan the QR code

an e-mail from a public authority (for example HZZO, Ministry, etc.) in which you are informed that you are entitled to the payment of assistance or reimbursement of expenses in a certain amount, and in order to be paid the same, you need to click on the link or scan the QR code

an e-mail from the Police Administration informing you that you have been accused of various criminal offenses and that you must submit your statement about the criminal offense within a certain period of time

How to recognize fraud?

Be sure that public authorities will not ask for your credit card information

Check the e-mail address of the sender, if it does not match the official e-mail address (domain) of the public authority, it is a fraud

Pay attention to grammatical and spelling mistakes, often such messages and letters are full of mistakes

You are invited to react urgently (within 24 to 72 hours) - click on the link, scan the code or report the crime within a certain time limit

Scanning QR codes or accessing a link opens a fake website that looks like the real one - pay attention to the URL!

If you receive a suspicious e-mail, follow the steps listed and do not click on links, do not scan QR codes, do not download attachments and do not respond to such messages!

Examples of phishing emails:

Photo source: cert.hr

Photo source: MoI of the Republic of Croatia

EXAMPLE 3. BUYING AND SELLING THROUGH INTERNET ADVERTISERS

You advertised a mobile phone for sale via an online classifieds or social network and a potential buyer soon contacted you

with a message. In the message, he states that he is interested in buying and asks if the item is still available. You are happy that you have found a customer and that you will make money, but first check whether the potential customer is really a customer or is trying to get your personal and financial information.

Frauds that occur when buying or selling an item that is advertised through online classifieds are very common, because attackers follow the ads that are published, but also publish fake ads in order to achieve financial benefit. We present an overview of how you will recognize that it is a fraud.

How to recognize fraud?

After the attacker confirms that he will buy the item, he will most likely say that he will immediately pay the funds and arrange for delivery. You will notice that he did not ask you for payment information (name and surname, account IBAN).

He will then provide you with a link and ask you to click on it and enter the required information in order to ensure the delivery of the item to your address and the receipt of funds to your account. It is very likely that a fake website will open that looks like a delivery service or classifieds website.

When you open the link, you will notice that you are asked to enter your credit card information. Keep in mind that only the first and last name of the account owner and the account's IBAN are required to deposit funds into the account. If you notice that someone is asking you for card information, it is a fraud! Do not enter data!

The attacker will insist that you fill in the information via the link because that's the only way the "paid" funds can reach your account.

If you notice a message like this, block the number, do not open links and do not enter your data!!

If you buy through online classified ads, do not open links and do not enter card information! Remember, for the payment of funds to the account of a natural person, information about the name and surname of the account owner and the IBAN of the account is sufficient. If the other party asks you to enter your card information in order to pay you funds, the word is fraud!

Example 4. FAKE EMAIL or SMS FROM A POSTAL AND DELIVERY SERVICES SERVICE

Attackers often use delivery services to obtain personal information and financial gain. Therefore, below we list several examples of fake messages in which the attacker wants to get you to pay money and leave your personal information:

An e-mail informing you that the package is waiting for delivery, and in order for it to be delivered, you need to pay a delivery fee of a few cents via a link. By clicking on the link, a fake page of the delivery service will open, and most often there will be a

notice stating that delivery is not possible and that a fee must be paid, otherwise the shipment will be returned to the sender.

An email informing you that your package will be returned to sender if you do not collect it and asking you to click on a link for more information. By clicking on the link, a fake page of the delivery service will open and there will be a notice stating that it is necessary to pay the postage fee within a certain period of time, otherwise the shipment will be returned to the sender.

An email informing you that your package cannot be delivered until customs and/or VAT fees are paid by clicking on the link. Clicking on the link will open a fake page of the delivery service and there will be a notice that you need to pay a fee in order to receive your shipment.

How to recognize fraud?

Check the sender, if it does not match the official e-mail address (domain) of the delivery service, it is a fraud

If you have received a link, please check whether it matches the official web address. Always check the link first by passing the mouse over the link and it should appear, but do not click. It is also possible to check the address by right-clicking and copying the address of the link into, for example, Word, then comparing the address with the official address.

Opening the link will most often open a fake website of the delivery service, check the URL address!

If you are asked to enter credit card information, do not enter the information, close the page and delete the e-mail or SMS.

Protect your personal information and do not share it lightly!