Piece of advice for the entrepreneurs – how not to fall for the Business E-mail Compromise fraud

A type of fraud initiated by a business e-mail compromise is well known worldwide. Potential victims of this fraud in Croatia are the companies that fail to verify the authenticity of their business correspondence, especially the ones doing business with foreign partners.

Frauds initiated by business e-mail compromise start by the scammers "**infiltrating" the e-mail correspondence**. Then, at the time scheduled for payment of certain goods or services, they send a fraudulent message formed in such a way that it cannot be easily differentiated from the preceding messages exchanged between the involved companies when arranging and carrying out this business transaction.
The scammers introduce themselves as employees of the company that is owed a certain amount for an ordered product or service, claiming that the bank and account number to be credited have changed in the meantime. In their message, they provide new account information and instruct the victim to make the payment to that account.

Importance of verifying authenticity

It is relatively easy to protect oneself from this kind of crime, provided the rules for checking of authenticity of business correspondence are strictly and constantly adhered to.
The personnel in charge of payment of invoices, or working in accounting firms that the payment of invoices is outsourced to, must verify the authenticity and accuracy of each e-mail they receive and where their business partners notify them about a change of the bank and the account that the payment for the purchased goods is to be made to, and this verification must be made by telephone and/or video conference call before initiating of the payment.
If they establish that it is a case of business e-mail account compromise, they are obligated to inform the Ministry of Interior by filing a report at the nearest police station.

How do the scammers get hold of the information?

Usually, scammers find out the name of a certain person. How do they do that? Most often, by the so-called social engineering: collecting of data from social networks and off the target company's web site, intercepting of the incoming mail, or even eavesdropping in establishments where the employees of such company gather during lunch break or after work.
After that, the specific person receives a so-called spear-phishing e-mail. Once the unsuspected target activates the malicious software by recklessly clicking on the link provided in the e-mail or on the infected file attached to such e-mail, the hacker gains

access to the target's computer. This is only one way the attackers operate, whilst another type of attack is carried out in a way that the insidious malicious software forwards all the e-mails from the Sent Items file directly to the mailbox created by the attacker specifically for that purpose.
As explained above, having analysed those e-mails, the hacker composes a false e-mail that the victim cannot discern from other e-mails exchanged with the partner with whom he/she usually communicates about payments of their invoices.

Companies having suppliers abroad as usual targets

The malicious software used in these attacks is extremely sophisticated, and hackers go the extra mile designing and fine-tuning it so carefully to ensure that it goes unnoticed by most anti-virus programs, or even using special remote access tools that the anti-virus programs will not recognise as a threat.
Globally, the Business E-mail Compromise is not a new type of fraud, with most frequent occurrences in the United States and in the Western Europe, and mostly targeting the companies regularly doing business abroad. The banks they chose to receive the payments to are mostly located in China.

Brochures with details of the most common types of online frauds:

- CEO / Business e-mail compromise (BEC) fraud
- Invoice fraud
- Bank phishing emails
- Bank vishing calls
- Bank smishing SMSs

otpbanka

CEO/BUSINESS EMAIL COMPROMISE (BEC) FRAUD

CEO/BEC fraud occurs when an employee authorised to make payments is tricked into paying a fake invoice or making an unauthorised transfer out of the business account.

HOW DOES IT WORK?

A fraudster calls or emails posing as a high ranking figure within the company (e.g. CEO or CFO).

They have a good knowledge about the organization.

They require an urgent payment.

They use language such as: 'Confidentiality', 'The company trusts you', 'I am currently unavailable'.

They refer to a sensitive situation (e.g tax control, merger, acquisition).

Often, the request is for international payments to banks outside Europe.

The employee transfers funds to an account controlled by the fraudster.

Instructions on how to proceed may be given later, by a third person or via email.

The employee is requested not to follow the regular authorisation procedures.

WHAT ARE THE SIGNS?

- Unsolicited email/phone call
- Direct contact from a senior official you are normally not in contact with
- Request for absolute confidentiality
- Pressure and a sense of urgency
- Unusual request in contradiction with internal procedures
- Threats or unusual flattery/promises of reward

WHAT CAN YOU DO?

AS A COMPANY

Be aware of the risks and ensure that **employees are informed and aware too**.

Encourage your staff to **approach payment requests with caution**.

Implement internal protocols concerning payments.

Implement a procedure to verify the legitimacy of payment requests received by email.

Establish **reporting routines** for managing fraud.

Review information posted on your company website, **restrict information and show caution** with regard to social media.

Upgrade and update technical security.

Always contact the police in case of fraud attempts, even if you did not fall victim to the scam.

AS AN EMPLOYEE

Strictly apply the security procedures in place for payments and procurement. **Do not skip any steps and do not give in to pressure**.

Always **carefully check email addresses** when dealing with sensitive information/money transfers.

In case of doubt on a transfer order, **consult a competent colleague**.

Never open suspicious links or attachments received by email. Be particularly careful when checking your private email on the company's computers.

Restrict information and show caution with regard to social media.

Avoid sharing information on the company's hierarchy, security or procedures.

If you receive a suspicious email or call, always inform your IT department.

EUROPOL EC3 European Cybercrime Centre

EBF European Banking Federation

#CyberScams

otpbanka

INVOICE FRAUD

HOW DOES IT WORK?

- A business is approached by somebody pretending to represent a supplier/service provider/creditor.
- A combination of approaches can be used: telephone, letter, email, etc.
- The fraudster requests that the bank details for a payment (i.e. bank account payee details) of future invoices be changed. The new account suggested is controlled by the fraudster.

WHAT CAN YOU DO?

AS A BUSINESS

Ensure that **employees are informed and aware** of this type of fraud and how to avoid it.

Instruct staff responsible for paying invoices to **always check them for any irregularities**.

Implement a **procedure to verify** the legitimacy of payment requests.

Review information posted on your company website, in particular contracts and suppliers. Ensure your staff limit what they share about the company on their social media.

AS AN EMPLOYEE

Verify all requests purporting to be from your creditors, especially if they ask you to change their bank details for future invoices.

For payments over a certain threshold, **set up a procedure to confirm** the correct bank account and recipient (e.g. a meeting with the company).

Do not use the contact details on the letter/fax/email requesting the change. Use those **from previous correspondence** instead.

When an invoice is paid, **send an email to inform the recipient**. Include the beneficiary bank name and the last four digits of the account to ensure security.

Set up designated Single Points of Contact with companies to whom you make regular payments.

Restrict information that you share about your employer on social media.

Always contact the police in case of fraud attempts, even if you did not fall victim to the scam.

EUROPOL EC3 European Cybercrime Centre

EBF European Banking Federation

#CyberScams

otpbanka

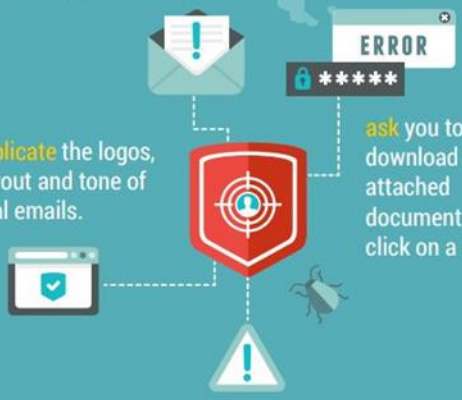
BANK PHISHING EMAILS

Phishing refers to fraudulent emails that trick the receivers into sharing their personal, financial or security information.

HOW DOES IT WORK?

These emails:

may look identical to the types of correspondence that actual banks send.



replicate the logos, layout and tone of real emails.

ask you to download an attached document or click on a link.

use language that transmits a sense of urgency.

WHAT CAN YOU DO?

- **Keep your software updated,** including your browser, antivirus and operating system.
- Be especially **vigilant** if a 'bank' email requests sensitive information from you (e.g. your online banking account password).
- **Look at the email closely**: compare the address with previous real messages from your bank. Check for **bad spelling and grammar.**
- **Don't reply to a suspicious email,** instead forward it to your bank by typing in the address yourself.
- **Don't click on the link or download the attachment,** instead type the address in your browser.
- When in doubt, **double check** on your bank's website or give the bank a call.

Cybercriminals rely on the fact that people are busy; at a glance, these spoof emails appear to be legitimate.

#CyberScams

Watch out when using a mobile device. It might be harder to spot a phishing attempt from your phone or tablet.

EUROPOL EC3 European Cybercrime Centre

EBF European Banking Federation

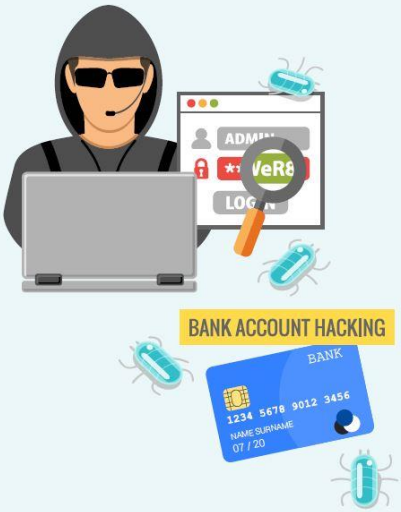
otpbanka

BANK VISHING CALLS

Vishing (a combination of the words Voice and Phishing) is a phone scam in which fraudsters try to trick the victim into divulging personal, financial or security information or into making a financial transfer to them.

WHAT CAN YOU DO?

- **Be wary** of unsolicited telephone calls.
- **Take the caller's number** and advise them that you will call them back.
- In order to validate their identity, **look up the organisation's phone number** and contact them directly.
- Don't validate the caller using the phone number they have given you (this could be a fake or spoofed number).
- Fraudsters can find your basic information online (e.g. social media). **Don't assume a caller is genuine** just because they have such details.
- **Don't share** your credit or debit card PIN number or your online banking password. Your bank will never ask for such details.
- **Don't transfer money** to another account on their request. Your bank will never ask you to do so.
- If you think it's a bogus call, **report it to your bank.**



EUROPOL EC3 European Cybercrime Centre

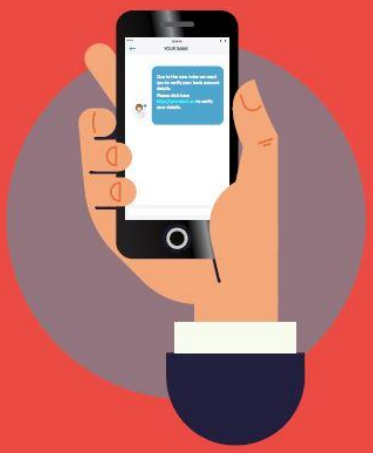
EBF European Banking Federation

#CyberScams

otpbanka

BANK SMISHING SMSs

Smishing (a combination of the words SMS and Phishing) is the attempt by fraudsters to acquire personal, financial or security information by text message.



HOW DOES IT WORK?

The text message will typically ask you to click on a link or call a phone number in order to 'verify', 'update' or 'reactivate' your account. But...the link leads to a bogus website and the phone number leads to a fraudster pretending to be the legitimate company.

WHAT CAN YOU DO?

- **Don't click on links, attachments or images** that you receive in unsolicited text messages without first verifying the sender.
- **Don't be rushed.** Take your time and make the appropriate checks before responding.
- **Never respond to a text message message** that requests your PIN or your online banking password or any other security credentials.
- If you think you might have responded to a smishing text and provided your bank details, contact your bank immediately.

EUROPOL EC3 European Cybercrime Centre

EBF

#CyberScams