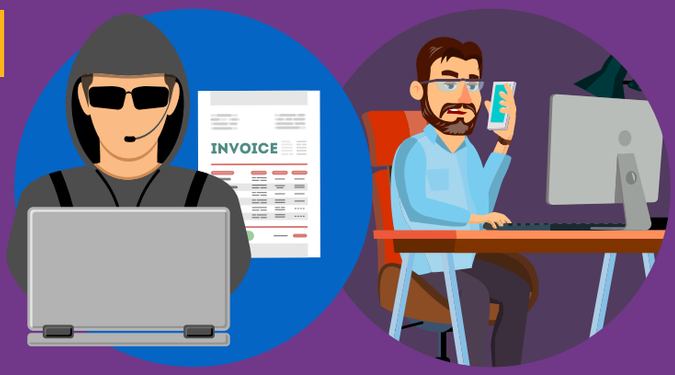
MASHTRIMET ME FATURAT



SI FUNKSIONON?

- Një biznesi i paraqitet dikush që pretendon se përfaqëson një furnizues/ofrues shërbimi /kreditor.
- Mund të përdoren disa mënyra paraqitjesh: telefon, letër, e-mail, etj.
- Mashtruesi kërkon që detajet bankare të pagesës së një fature të ardhshme (psh. detajet e llogarisë bankare për pagesën) të ndryshohen. Llogaria e re e sugjeruar kontrollohet nga mashtruesi.

ÇFARE MUND TE BENI?

SI BIZNES

Sigurohuni që punonjësit janë të informuar dhe të vetëdijshëm mbi këtë lloj mashtrimi dhe si ta shmangin atë.

Udhëzoni stafin përgjegjës për kryerjen e pagesave t'i kontrollojnë ato për çdo parregullsi.

Implementoni një procedurë për të verifikuar legjitimitetin e kërkesave për pagesa.

Rishikoni informacionet e postuara në faqen zyrtare të kompanisë suaj, në veçanti kontratat dhe furnizuesit. Sigurohuni që stafi juaj të limitohet mbi çfarë poston në mediat sociale.

SI PUNONJES

Verifikoni çdo kërkesë që pretendohet të vijë nga kreditorët, veçanërisht nëse kërkojnë të ndryshohen detajet e tyre bankare për faturat e ardhshme.

Për pagesa mbi një limit të caktuar, krijoni një procedurë për të konfirmuar detajet e sakta bankare dhe përfituesin (p.sh. një takim me kompaninë).

Mos përdorni detajet e kontaktit në letër/faks/e-mail që kërkon ndryshimin. Përdorni kontaktet e korrespondencave të mëparshme.

Kur një faturë paguhet, dërgoni një e-mail duke informuar përfituesin. Përfshini detaje mbi bankën marrëse dhe katër shifrat e fundit të llogarisë për të garantuar siguri.

Krijoni pika të caktuara kontakti me kompanitë me të cilat kryeni pagesa të rregullta.

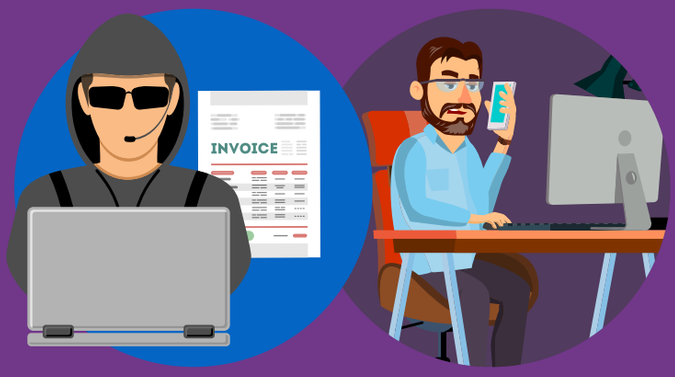
Limitoni informacione/detaje mbi punëdhënësin tuaj në mediat sociale.

! Kontaktoni policinë për çdo tentativë mashtrimi edhe nëse nuk jeni viktimë e tyre.

EUROPOL EC3 European Cybercrime Centre | EBF European Banking Federation | INTESA SANPAOLO BANK Albania

#CyberScams

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 postedn 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 thosefrom 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 | INTESA SANPAOLO BANK Albania

#CyberScams