MASHTRIMI ME E-MAIL PER KRYERJE PAGESASH

Mashtrimet nëpërmjet e-mail-it ndodhin kur një punonjës i autorizuar për të bërë pagesat është mashtruar për të paguar një faturë të rreme që i ka ardhur nëpërmjet e-mail ose kryerjen e një transferimi të paautorizuar nga një biznes.

SI FUNKSIONON?

Mashtruesi telefonon ose dërgon e-mail si një drejtues i lartë i kompanisë (psh: CEO ose CFO).

Ka njohuri të mira për kompaninë .

Kërkojnë një pagesë urgjente.

Përdorin terma si:: 'Konfidenciale', 'Kompania ka besim te ty', 'Jam përkohësisht i padisponueshëm'.

Shpesh, kërkesa bëhet për pagesa drejt bankave ndërkombëtare jashtë Europës.

Punonjësi transferon fonde në një llogari që kontrollohet nga mashtruesi.

Udhëzimet se si do të procedohet mund të jepen më pas nga një person i tretë ose nëpërmjet e-mail.

Punonjësit i kërkohet të mos ndjek procedurat e zakonshme të autorizuara.

I referohen një situate delikate (p.sh: kontrolli i taksave, bashkim kompanish, blerje).

CILAT JANE SHENJAT DALLUESE?

- Telefonatë/e-mail i papritur
- Kontakt i drejtpërdrejtë nga një drejtues i lartë i kompanisë që nuk keni kontakt zakonisht
- Kërkojnë konfidencialitet të plotë
- Ushtrohet presion e kërkohet të veproni me urgjencë
- Kërkesa është e pazakontë dhe në kundërshtim me procedurat e bankës
- Kërcënoheni ose ju premtohet shpërblim i pazakontë

ÇFARE MUND TE BESH?

KOMPANIA

Njihni rreziqet dhe sigurohu që punonjësit janë të informuar dhe i njohin rreziqet gjithashtu.

Inkurajoni stafin që të tregojë kujdes gjatë kryerjes së pagesave.

Implementoni protokolle të brendshme në lidhje me pagesat.

Hartoni procedura për verifikimin e pagesave që kërkohen nëpërmjet e-mail.

Vendosni rutinë raportimesh për të menaxhuar mashtrimet.

Rishikoni informacionin e vendosur në faqen e internetit, të kufizojë dhe rishikojë informacionin e publikuar në mediat sociale.

Përmirësoni dhe përditësoni sigurinë teknike.

Kontaktoni policinë në rastet e përpjekjeve për mashtrim dhe nëse nuk bini viktimë e mashtrimit.

PUNONJESI

Zbatoni rreptësisht procedurat e sigurisë për pagesat dhe prokurimet. Mos kapërceni asnjë hap të procedurave dhe të mos bini pre e presionit.

Kontrolloni gjithmonë me kujdes adresat e e-mail që kanë të bëjnë me informacione të ndjeshme ose transferta parash.

Në rast dyshimi për një urdhër transferimi, konsultohuni me një koleg kompetent.

Mos klikoni link ose dokumenta bashkëngjitur në e-mail. Jini veçanërisht i kujdesshëm kur kontrolloni e-mail privat në kompjuterat e Bankës.

Tregoni kujdes dhe të kufizoni informacionin që publikoni në mediat sociale.

Shmangni ndarjen e informacionit që lidhet me punën e Bankës, hierarkinë, sigurinë ose procedurat.

Informoni departamentin e Sigurisë së Informacionit nëse merrni një e-mail apo telefonatë të dyshimtë.

EUROPOL EC3 European Cybercrime Centre

EBF European Banking Federation

INTESA SANPAOLO BANK Albania

#CyberScams

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).

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

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

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

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

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

INTESA SANPAOLO BANK Albania

#CyberScams