Kujdes nga kriminelët që pretendojnë të jenë WHO

Kriminelët po maskojnë veten si WHO për të vjedhur para ose informacione të ndjeshme. Nëse kontaktoheni nga një person ose organizatë që duket se është nga OBSH, verifikoni vërtetësinë e tyre përpara se të përgjigjeni.

Organizata Botërore e Shëndetit :

- kurrë nuk kërkon nga ju të identifikoheni për të parë informacionin e sigurisë dhe asnjëherë me email nuk bashkëngjit linke per ti klikuar.
- kurrë nuk kërkon nga ju që të vizitoni një link jashtë www.who.int
- kurrë nuk ngarkon para për të aplikuar për një vend pune, të regjistroheni në një konferencë ose të rezervoni një hotel
- kurrë mos bën llotari ose ofron çmime, grante, çertifikata ose fonde përmes emailit
- kurrë nuk kërkon nga ju të dhuroni direkt në planet e reagimit emergjent ose në apelet e financimit.

Kujdes që kriminelët përdorin email, uebfaqe, telefonata, mesazhe me tekst, dhe madje edhe mesazhe faksi për mashtrimet e tyre.

Ju mund të verifikoni nëse komunikimi është i ligjshëm duke kontaktuar drejtpërdrejt WHO.

Kontaktoni OBSH

Raportoni një mashtrim

Phishing: emailet me qëllim të keq duket se janë nga OBSH

OBSH është në dijeni të mesazheve të dyshimta me email, që përpiqen të përfitojnë nga urgjenca e koronavirusit . Ky veprim mashtrim quhet phishing.

Këto emaile "Phishing" duket se janë nga OBSH, dhe do t'ju kërkojnë të:

- jepni informacion të ndjeshëm, siç janë emrat e përdoruesve ose fjalëkalimet
- klikoni në një lidhje me qëllim të keq
- hapni një shtojcë dashakeqe.

Duke përdorur këtë metodë, kriminelët mund të instalojnë malware ose të vjedhin informacion të ndjeshëm.

Si të parandaloni phishing:

- Verifikoni dërguesin duke kontrolluar adresën e tyre të postës elektronike.
- Sigurohuni që dërguesi të ketë një adresë e-mail si "person@who.int" Nëse ka ndonjë gjë tjetër përveç "kush.int" pas simbolit ‘@", ky dërgues nuk është nga OBSH.
- OBSH nuk dërgon email nga adresat që përfundojnë në ‘@ who.com ',‘ @ who.org' ose ‘@ who-safety.org 'për shembull.
- Kontrolloni lidhjen para se të klikoni.
- Sigurohuni që lidhja fillon me ‘https://www.who.int '. Më mirë akoma, lundroni drejtpërdrejt në uebfaqen e WHO, duke shtypur ‘https://www.who.int 'në shfletuesin tuaj.
- Kini kujdes kur jepni informacione personale.

- Gjithmonë konsideroni pse dikush dëshiron informacionin tuaj dhe nëse është i përshtatshëm. Nuk ka asnjë arsye që dikush do të duhet emrin e përdoruesit dhe fjalëkalimin tuaj për të hyrë në informacionin publik.
- Mos nxitoni ose mos u ndjeni nën presion.
- Kriminelët kibernetikë përdorin raste urgjente siç është 2019-nCov për t'i marrë njerëzit të marrin vendime shpejt. Gjithmonë merrni kohë për të menduar për një kërkesë për informacionin tuaj personal, dhe nëse kërkesa është e përshtatshme.
- Nëse keni dhënë informacion të ndjeshëm, mos u frikësoni.
- Nëse besoni se keni dhënë të dhëna të tilla si emrin e përdoruesit ose fjalëkalimet për kriminelët në internet, ndryshoni menjëherë letrat kredenciale në secilën faqe ku i keni përdorur ato.
- Nëse shihni një mashtrim, raportojeni.