ORDRE DES MEDECINS
CONSEIL NATIONAL

ORDE DER ARTSEN
NATIONALE RAAD

Voorzichtigheid van de arts tegenover cybercriminaliteit

Doc	a170006
Publicatiedatum	25/02/2023
Origine	NR
Thema's	Internet Informatica

De nationale raad van de Orde der artsen werd onlangs op de hoogte gebracht van een nieuwe vorm van fraude tegenover artsen met behulp van via het internet verkregen informatie.

Een persoon met slechte bedoelingen neemt de reviews door op de online beroepspagina's van een arts om de identiteit van één van zijn patiënten te achterhalen. Vervolgens wordt de arts in kwestie opgebeld door een persoon die zich voordoet als apotheker aan wie de patiënt, geïdentificeerd via de beroepspagina, gevraagd zou hebben hem een geneesmiddel te verstrekken waarvoor een voorschrift nodig is (diazepam, zolpidem, enz.). Onder verscheidene voorwendselen (geen kleine verpakking, het eHealth-platform ligt plat, het INSZ-nummer werd verkeerd genoteerd) wordt de arts gevraagd een grote verpakking van het geneesmiddel voor te schrijven en mondeling de voorschriftcodes en het INSZ-nummer van de patiënt mee te delen.

Dit voorbeeld maakt dus duidelijk dat artsen niet gespaard blijven van cyberfraude in allerlei vormen en benamingen (phishing, vishing, smishing, brandjacking, defacing, formjacking, angler phishing, spearphishing, spoofing, enz.).

Artsen moeten aandacht hebben voor digitale veiligheid, zowel wat de beveiliging van hun informaticamateriaal betreft als hun goede aanpak van de risico's en aanvallen.

Het is niet alleen in hun belang maar ook in dat van de patiënten van wie zij gegevens verwerken dat zij zich beschermen tegen cybercriminaliteit.

Naleving van het veiligheidsbeleid dat in de professionele omgeving, met name in zorginstellingen, werd ontwikkeld, is essentieel.

De nationale raad spoort de artsen ertoe aan kennis te nemen van de goede praktijkvoering inzake preventie en melding te maken van fraude waarvan zij het slachtoffer zijn.

Het Centrum voor Cybersecurity België (CCB) is de nationale autoriteit voor cyberveiligheid in België (opgericht bij koninklijk besluit van 10 oktober 2014). Hun website bevat heel wat nuttige informatie, onder meer in de vorm van webinars

(https://ccb.belgium.be/nl/work).

Via de website Safeonweb.be informeert het CCB internetsurfers over online veiligheid en wat te doen in geval van een probleem

(https://www.safeonweb.be/index.php/nl/tips; (https://www.safeonweb.be/nl/eerste-hulp).

De website van het federale Cyber Emergency Response Team (CERT.be), de operationele dienst van het Centrum voor Cybersecurity België (CCB), verstrekt niet alleen tips maar bevat ook een pagina om incidenten te melden (https://cert.be/nl).

De website van de federale politie behandelt eveneens vragen over cyberpreventie (https://www.politie.be/5998/nl/vragen/cyberpreventie).

Wij wijzen u op enkele basisregels die gevolgd dienen te worden :

- controleer de kwetsbaarheid van uw computermateriaal ;
- gebruik verschillende en sterke paswoorden
- geef uw identificatiegegevens, wachtwoorden of geheime codes niet door via telefoon of mail ;
- behandel elk verzoek om vertrouwelijke informatie met argwaan en controleer de wettigheid van uw gesprekspartner ;
- let op voor ongevraagde berichten, vooral als ze niet persoonlijk zijn, dringende actie vereisen, of uw nieuwsgierigheid willen wekken (“kijk wat ik over u gelezen heb”…) of een dreigende toon aannemen ;
- klik niet op links in ongevraagde berichten ;
- klik niet op links en open geen bijlagen waarin u geen vertrouwen hebt ;
- behandel officiële berichten met tikfouten of een atypische formulering met argwaan (ga naar de officiële website om de informatie te controleren of neem contact op) ;
- lees het adres van de afzender aandachtig, frauduleuze mails gebruiken vaak een adres dat lijkt op een betrouwbaar adres maar met een letter op een andere plaats of een verkeerde domeinnaam ;
- behandel aanbiedingen « die te mooi om waar te zijn » met argwaan ;
- wees u ervan bewust dat sociale media zinvolle informatie bevatten om phishing persoonlijker te maken ;
- informeer u regelmatig over cyberveiligheid.

Opmerking :

Bij phishing wordt een vals bericht gestuurd naar tal van accounts. Het doelwit wordt gevraagd een bestand te downloaden of te openen, zijn persoonsgegevens mee te delen, een bijlage te openen, met als doel een cyberaanval in te zetten (gegevenslek, ransomware, enz.). Phishing kan gebeuren via e-mail maar ook via sms (smishing) of berichten op social media.

Vishing is een vorm van phishing via een telefonische oproep.

Spearphishing is een meer doelgerichte en persoonlijke versie van phishing. De crimineel identificeert zijn slachtoffer en zoekt persoonlijke informatie over hem op om aldus een bericht aan te maken dat er authentiek uitziet en van een vertrouwensbron lijkt te komen.

Angler phishing is een vorm van phishing gericht op de accounts van social media. Hackers geven zich uit voor een medewerker van de klantendienst van deze social media (social phising).

Spoofing is een vorm van bedrog waarbij de fraudeurs de identiteit van een andere persoon aannemen om het vertrouwen te winnen van het doelwit. Ze doen zich voor als medewerker van een bank, een openbare dienst of een andere bekende organisatie.

Bij brandjacking laat de fraudeur zich doorgaan voor een bekend bedrijf, een groot merk of een beroemd persoon.

Formjacking richt zich op online winkelen. Het heeft tot doel de achterliggende software van een

webwinkel bijvoorbeeld binnen te dringen om er malware te installeren.

Bij defacing wordt de inhoud van een webpagina vervangen door een activistische boodschap of content die het imago van het bedrijf schade toebrengt. Hackers beletten de toegang tot de website om losgeld te verkrijgen, trachten gevoelige gegevens te stelen, enz.