VUB Informatieveiligheid en Privacy

How To – Herken Vhishing, Phishing en Smishing

Verantwoordelijke:
Chief Information Security Officer

Contact(en):
ciso@vub.be

Laatste update:
30 maart 2020

I. Overzicht

Een “How To …” document geeft informatie en/of hints en tips over een specifiek Informatieveiligheid en Privacy (IVP) onderwerp. Het bevat geen dwingende standaard/richtlijn, het geeft info over hoe een standaard/richtlijn kan toegepast worden.

Het is een ‘levend’ document en de kwaliteit is deels afhankelijk van de feedback van zijn lezers/gebruikers. De cover bladzijde geeft het contact e-mailadres waarnaar feedback kan gestuurd worden

Een “How To” document volgt geen formeel advies en goedkeuringsproces.

II. Herken Vhishing, Phishing en Smishing

II.1. Hoe herken ik Phishing, Vhishing en Smishing?

Cybercriminelen proberen steeds vaker gevoelige gegevens aan je te ontfutselen via valse e-mails, websites of berichten. Om te vermijden dat ze bij jou kunnen toeslaan geven we enkele tips om dit soort berichten te herkennen. Want de beste beveiliging tegen computeraanvallen begint bij je zelf!

Via e-mail (‘phishing)’, telefoon (‘voice phishing’, of ‘vishing’) of sms (‘smishing’) vissen criminelen naar gevoelige informatie zoals wachtwoorden, gebruikersnamen of bankgegevens. Een veelgebruikte tactiek daarbij is om misbruik te maken van informatie die jou in eerste instantie heel betrouwbaar en bruikbaar lijkt. Maar hoe herken je een verdacht bericht?

II.1.1. De afzender

Stel jezelf vragen rond de afzender van een verdachte mail of telefoon: Ken je hem? Had je al eerder contact met hem? Kreeg je echt een eerste aanmaning tot betaling? Ken je die 'vriend in nood' wel? Is zijn mailadres correct? Let op: zelfs een legitiem e-mailadres is geen garantie op betrouwbaarheid.

II.1.2. De bestemmeling(en)

Kijk ook naar de bestemmeling(en) (en mensen in cc) van de e-mail. Als de mail verzonden werd naar een ongebruikelijke groep mensen die niets gemeen hebben of die je niet kent, wees dan extra voorzichtig. Zit het bericht in je spam/junk folder? Wees dan extra voorzichtig.

II.1.3. De verzendingsdatum

Ontving je een mail, die normaal gezien tijdens werkuren zou worden verzonden, op een ongewoon tijdstip, zoals 3u ‘s morgens? Wees dan extra alert.

II.1.4. Het onderwerp

Kijk na of het onderwerp van de mail aansluit bij de inhoud van het bericht en of het bericht zogezegd een antwoord is op een mail die je echter zelf nooit verstuurd hebt (voorvoegsel « RE: » bij het begin van het onderwerp).

II.1.5. De inhoud van de mail

Kijk of de inhoud van de boodschap wel zinvol is. Een officiële instantie zal nooit via e-mail, sms of telefoon vragen om je wachtwoord, bankgegevens of persoonlijke gegevens. Ook spellings- en grammaticafouten zijn vaak een indicator van een verdacht bericht. Berichten met algemene en vage aanspreektitels, of je e-mailadres als aanspreking, wantrouw je beter.

II.1.6. De (hyper)links

Hyperlinks kunnen zeer gevaarlijk zijn. Vaak vraagt de afzender om een bijlage te openen maar klikken op één verdachte link kan een hele organisatie in gevaar brengen! Een verdachte link kan je het best ontmaskeren door je computermuis erover te bewegen **zonder** erop te klikken: het volledige adres wordt dan weergegeven. Verwijst dit naar een ander webadres, dan is dit gevaarlijk! Is de domeinnaam ook echt de naam van de organisatie?

Zo is bij de link www.safeonweb.be/tips het domein 'safeonweb.be' en bij de link www.safeonweb.tips.be/safeonweb is 'tips.be' het domein en word je naar een andere website geleid.

II.1.7. De bijlagen

Grootste risicofactor, en het vaakst gebruikt door hackers, is een aangetaste bijlage. Als je geen bijlage verwacht, open die dan niet! Enkel van bestanden die eindigen op « .txt » kan met zekerheid gezegd worden dat ze geen virussen bevatten. Alle andere documenten, zoals Excel- of PowerPoint-bestanden, kunnen besmet zijn!

II.1.8. Smishing

Steeds vaker wordt sms gebruikt om berichten te versturen die valse links bevatten met de bedoeling mensen op te lichten. Deze vorm van phishing kreeg zelfs een naam: smishing of ook SMS-phishing. Ook hier geldt: klik niet op de link. Als je dit toch gedaan hebt, vul de velden verder niet in en breek elke interactie af. Als je tijdens een telefonisch contact met de oplichters toch tot betaling bent over gegaan, contacteer je bank en doe aangifte bij de politie.

II.2. Wat als?

Als je toch je VUB-gebruikersnaam en/of -wachtwoord hebt gegeven, verander onmiddellijk je paswoord en verwittig de helpdesk@vub.be

Gaf je bankgegevens door, contacteer dan meteen je bank en blokker je kaart via CardStop (https://cardstop.be/en/home.html).

.1. Wat als je twijfelt?

Klik nooit op een link of bijlage. Denk je dat het een poging is om te infiltreren, verwijder dan de mail uit je mailbox door de toetsen « Shift » en « Del » tegelijk in te drukken en contacteer de afzender als je hem kent. Komt het bericht niet van vrienden, laat hen dan via telefoon, sms of social media weten dat hun account gehackt is. Bij sommige sociale netwerken kan je berichten als 'vals' markeren. Bij organisaties of bedrijven ga je naar hun site en controleer je of die zogenaamde 'dringende' actie bestaat. Vind je niets terug, dan kan je ook naar hen bellen.

Valse berichten, ook valse sms-berichten, kan je doorsturen naar helpdesk@vub.be.

.2. Office 365

Om het rapporteren van Phishing door Office 365 gebruikers eenvoudiger te maken, werd er een 'button' toegevoegd aan Outlook (zowel desktop als mobiele versie) en de online webmail:

U selecteert de e-mail in het overzicht en klikt op deze button. De verdachte e-mail wordt dan automatisch naar de helpdesk verstuurd. Deze zal u contacteren indien meer informatie nodig is.

.3. Extra waakzaamheid voor corona-berichten!

Steeds meer computerhackers maken misbruik van de gevolgen van het coronavirus. Zeker nu we door deze onzekere tijden uit onze comfortzone gehaald werden en we extra nood hebben aan informatie en aan sociale contacten. Hackers gebruiken daarom onderwerpen die ons emotioneel of professioneel bezighouden om zo hun malware binnen te smokkelen.

.3.1. *Kijk uit voor illegale versies van de interactieve kaart Johns Hopkins University*

Cybersecurity experts waarschuwen voor een programma waarmee je de evolutie van het virus op een wereldkaart kan volgen. Een dashboard van coronavirusinfecties en -doden van de Johns Hopkins University, wordt door kwaadaardige websites misbruikt om virussen te installeren die wachtwoorden kunnen detecteren en stelen. De installatie ervan gebeurt enkel als JavaScript is ingesteld.

Gebruik daarom enkel de officiële link https://coronavirus.jhu.edu/map.html.

.3.2. *COVID-19 Tracker App bevat ransomware*

De Android App COVID19 Tracker App waarmee je gevallen van COVID-19 kan opvolgen, is geïnfecteerd met de ransomware CovidLock. Deze gebruikt technieken om het slachtoffer de toegang tot zijn of haar telefoon te ontzeggen door een wijziging van het wachtwoord om de telefoon te ontgrendelen, te forceren. Hierna krijg je meteen een scherm te zien waarop uitgelegd wordt hoe je binnen de 48 uur $100 aan Bitcoin moet betalen. Wanneer je dat niet doet, wordt alle data van je toestel verwijderd en dreigt men om al je contacten, foto's, video's en alle sociale media accounts publiek te lekken op het internet.

Hou jezelf en de VUB veilig!

Je vindt de laatste informatie op ivp.vub.be