VUB Informatieveiligheid en Privacy

How To – Herken Vhishing, Phishing en Smishing

Verantwoordelijke:
Chief Information Security Officer

Contact(en):
ciso@vub.be

Laatste update:
17 oktober 2023 (v1.4)

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 Phishing, Vhishing 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?

II.2.1. Je gegevens hebt ingegeven?

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).

II.2.2. Wat als je twijfelt?

Klik nooit op een link of bijlage. Komt de e-mail (zogezegd) van een vriend, contacteer dan deze via een ander kanaal (bv., telefoon) zodat deze kan bevestigen of het om een echte of fraudeleuze e-mail gaat. 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.

Denk je dat het een poging is om te infiltreren, verwijder dan de e-mail uit je inbox en laat de afzender via telefoon, sms of social media weten dat de account gehackt is. Bij sommige sociale netwerken kan je berichten als 'vals' markeren.

II.2.3. Wat als je een phishing herkend hebt?

Om het rapporteren van Phishing door Office 365 gebruikers eenvoudiger te maken, werd er een 'button' toegevoegd aan de desk/laptop Outlook:

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.

Valse berichten kan je ook als bijlage (.EML extensie) e-mailen naar phishing@vub.be. Ook valse sms-berichten kan je naar phishing@vub.be sturen.

Hou jezelf en de VUB veilig!

Je vindt de laatste informatie op ivp.vub.be