ACHTERGRONDINFORMATIE

VZW SInt-Augustinusinstituut

voor:

SInt-Augustinusinstituut

Deze nota maakt deel uit van het informatieveiligheid- en privacybeleid (IVPB).

Versie	Datum	Status	Auteur(s)	Opmerking
1.0	2018-05-25	GELDIG	Bart Despiegelaere	

1 *Wachtwoordbeleid – Phishing: hengelen naar gegevens …*

1.1 Wat is phishing?

Je zal zelf weleens een e-mail hebben gekregen die leek te komen van de bank of het telecombedrijf waar je al dan niet klant bij bent. In de mail wordt meestal gevraagd om op een link te klikken en dan je persoonlijke gegevens zoals naam, pincode, bankgegevens, wachtwoord… in te vullen. Waarschijnlijk word je in de mail ook gevraagd om het snel te doen. De reden die de mail opgeeft zijn uiteenlopend maar klinken heel realistisch: bijvoorbeeld omdat je achterstaande betalingen hebt en je anders een boete krijgt, of omdat er verdachte activiteiten zijn opgemerkt omtrent het gebruik van je kredietkaart maar het kan ook gewoonweg gaan omdat we je gegevens willen controleren.
Het aanmanen om het snel te doen is wel heel cruciaal omdat jij dan gewoon minder snel nadenkt en sneller gaat 'bijten'.

Eens je echter op de link klikt, word je naar een valse website geleid die lijkt op het officiële portaal: een *gespoofte* website. Meestal een nagemaakte website met een adres dat enorm goed lijkt op de originele (voorbeeld zou zijn www.beltius.be i.p.v. www.belfius.be) Indien je daar je gegevens zou invullen, worden ze rechtstreeks naar een cybercrimineel gestuurd die uit is op jouw informatie. Het kan ook dat je via de link malware op je computer krijgt, zoals een keylogger die je informatie bijhoudt, of ransomware, die je bestanden of je volledige computer versleutelt.

Dat is een voorbeeld van phishing, maar het fenomeen beperkt zich allerminst tot die exacte situatie. Phishing is een vorm van social engineering waarbij een cybercrimineel gegevens of geld van een gebruiker probeert te stelen. En dat kan op heel veel verschillende manieren.

1.2 Soorten phishing

Phishing gebeurt meestal via e-mail, hoewel het ook via een app, valse website, of ook telefonisch kan. Hieronder de meest voorkomende soorten:

Spearphishing: Leunt erg aan bij standaardphishing, alleen gaat het hier niet om een willekeurig doelwit. *Een specifiek slachtoffer* wordt uitgekozen en het bericht wordt gepersonaliseerd om de persoon te doen geloven dat het om een legitieme boodschap gaat. Vaak doet men wat social engeneering om jouw te doen geloven dat de mail afkomstig is van je baas of van een bepaalde persoon uit je werkomgeving dienst die je vertrouwt.

Whaling: Spearphishing, maar dan gericht op de "grote vissen": managers, directeurs, CEO's, CFO's, en dergelijke. In plaats van één werknemer in de luren te leggen, mikt deze aanval op het groffe geld. De login-gegevens van de managers kunnen immers gebruikt worden om bedrijfskritische gegevens te stelen of phishing-mails naar honderden werknemers tegelijkertijd te sturen. Wie gaat er ooit een mail weigeren die effectief van de CEO komt?

Pharming: In plaats van te vissen, kiezen sommige cybercriminelen er ook voor om te oogsten. Met pharming worden nietsvermoedende gebruikers bij het surfen omgeleid worden. Dat kan bijvoorbeeld door een gehackte DNS-server. Zelfs wanneer de gebruiker dan de juiste url ingeeft, wordt hij nog omgeleid naar een valse website. Doelwitten zijn bijvoorbeeld de website van je bank, of van een sociaal netwerk. Wanneer je inlogt, zijn je gegevens niet langer privé.

1.3 Hoe herken je phishing?

Enkele jaren terug was het nog niet eens bijster moeilijk om een phishing-mail te herkennen, vooral niet in het Nederlands. De taal die werd gebruikt in de mail was vaak doorspekt met spelfouten en grammaticale flaters op een manier die zelfs de grootste taalbarbaar nauwelijks kon ontgaan. De huidige trend geeft echter aan dat cybercriminelen iets meer werk steken in de geloofwaardigheid van hun phishingmails. Veel van die mails zijn haast niet te onderscheiden van de *real deal*. Je kan wel een paar stappen overlopen om twijfel uit te sluiten.

Let op de begroeting: Rudimentaire phishing-mails die in bulk worden verzonden, beginnen vaak met een heel generische begroeting, zoals “Geachte klant” of “Beste collega”. Het is geen waterdicht signaal, aangezien spearphishing-mails wel gepersonaliseerd zijn, maar er moet een lampje gaan branden als het zo is.

Wat wordt er gevraagd: Een echte bank, telecombedrijf of andere instantie zal nooit via e-mail vragen om je gegevens te bevestigen, of andere informatie in te geven, via een link. Als het bovendien dringend moet, kan je ervanuit gaan dat ze zullen bellen.

Check de link: De link in phishing-mails beschrijft vaak de officiële pagina in de linktekst, maar leidt eigenlijk naar een heel andere website. Controleer de eindbestemming door over de link te zweven. Je kan de url dan linksonder in de hoek van je scherm bekijken.

Bij twijfel kan je altijd bellen naar de officiële instantie zelf. Doe dat dan aan de hand van een telefoonnummer dat je op een onafhankelijke website vindt, en dus niet het nummer dat eventueel in de mail te vinden is. Als je belt, kan de organisatie makkelijk zeggen of de mail legitiem is, of niet, en kunnen ze toekomstige klanten sneller waarschuwen voor frauduleuze e-mails.

2 *Communicatiebeleid – Nettiquette*

Bron: https://www.leren.nl/rubriek/computers_en_internet/internetten/nettiquette/

2.1 Wanneer wel e-mail, wanneer niet?

‘Uit onze administratie blijkt dat uw dienstverband bij de Rijksuniversiteit is beëindigd’. Dit bericht vonden de 7.000 medewerkers van de Rijksuniversiteit Groningen op een maandagochtend in november 2006 in hun mailbox. Gelukkig bleek het om 'fout’ in het computersysteem' te gaan. Waarom het automatisch gegenereerde mailtje naar duizenden medewerkers was gestuurd, was een groot raadsel. Nadat de fout was ontdekt, volgde meteen een excuusmail waarin de medewerkers werd verzekerd dat het een foutief bericht betrof en zij zich geen zorgen hoefden te maken over hun baan. De hele affaire had honderden bezorgde telefoontjes en e-mails tot gevolg.

Minder fortuinlijk waren de 400 medewerkers van een Amerikaanse elektronicaketen RadioShack in september 2006. Zij werden per e-mail op de hoogte gebracht van hun ontslag en konden meteen hun spullen pakken. ‘Omwille van de efficiency’, had de directie van het bedrijf voor deze werkwijze gekozen. De medewerkers waren woedend en vonden de werkwijze ‘onmenselijk en respectloos’.

E-mail is in lang niet elke situatie het juiste communicatiemiddel. Denk bijvoorbeeld aan zaken die iemand persoonlijk raken, zoals de beëindiging van een dienstverband. Dit hoort in een persoonlijk gesprek besproken te worden. Of als je een vraag hebt waar je meteen antwoord op wilt, kun je beter de telefoon pakken of even bij je collega langsgaan en het hem vragen. Toch wordt e-mail regelmatig gebruikt in situaties waarin een persoonlijk gesprek beter op zijn plaats was geweest. Niet zelden leidt dit - vaak ondoordacht – automatisme tot irritaties, woede en misverstanden. Vraag je bij elk bericht even af of het wel verstandig is voor de betreffende boodschap e-mail als medium te gebruiken.

Situaties waarin je e-mail kunt gebruiken

Je kunt je mail gebruiken als je:

- Een afspraak wilt maken met 1 of meerdere personen
- Een afspraak wilt bevestigen
- Een eenvoudige vraagt hebt
- Een vraag hebt waar je niet snel een antwoord op hoeft te krijgen
- Een antwoord moet geven op een eenvoudige vraag
- Aan veel mensen tegelijk een mededeling wilt doen (en die niet heel belangrijk is)
- Een vergadering wilt plannen
- Iemand wilt bereiken die heel slecht bereikbaar is.

Situaties waarin je e-mail beter niet kunt gebruiken

Je kunt je mail beter niet gebruiken als je:

- Een meningsverschil hebt
- Vertrouwelijke informatie wilt uitwisselen
- Slecht nieuws hebt
- In een situatie zit waar een probleem bestaat of dreigt te ontstaan
- Op het allerlaatste moment een vergadering of afspraak wilt afzeggen
- Veel vragen hebt
- Een vraag hebt waar je met spoed een antwoord op wilt hebben

- Vertrouwelijke informatie wilt uitwisselen
- Een vervelend bericht hebt.

Andere mogelijkheden

Wat kun je doen als e-mail niet het meest geschikte medium is?

- Loop bij je collega langs
- Pak de telefoon
- Maak een afspraak voor een persoonlijk gesprek
- Verstuur de informatie via de (interne) post
- Stuur een fax
- Spreek je collega aan in de kantine

2.2 Do's van emailen

Je typt een bericht, kiest een adres, drukt op verzenden en... klaar. Een kind kan de was doen. E-mail heeft haar populariteit te danken aan het gemak en de snelheid waarmee een berichtje kan worden verstuurd. Maar juist daardoor gaat het ook zo vaak mis: in de haast opgestelde berichten vol spelfouten, onduidelijke verzoeken en nutteloze mededelingen leiden tot irritatie, volle inboxen en veel tijdverlies, want al die e-mails moeten toch geopend en bekeken worden.

Wees helder en to the point

Verplaats je in de ontvanger van je e-mail en geef in de onderwerpregel bovenaan het bericht aan waar het over gaat. Je kunt bijvoorbeeld aangeven wat je van hem verlangt en - zonodig - wanneer. Ook kun je (duidelijk!) verwijzen naar eerdere e-mails. Bijvoorbeeld: '... in mijn mail van 24 september jl. met als onderwerp 'concept beleidsnota versie 1.2'. Het is dan voor de ontvanger meteen duidelijk of hij snel actie moet ondernemen of dat je bericht even kan wachten. Bovendien kan hij je bericht zo gemakkelijk terugvinden. Hiermee toon je niet alleen respect voor de tijd van een ander, je ontvangt waarschijnlijk ook een helder antwoord terug. Probeer je zoveel mogelijk tot één onderwerp te beperken. Heb je meerdere onderwerpen, spreid ze dan over meerdere e-mails. De ontvanger houdt zo het overzicht en kan je e-mails gemakkelijker afhandelen. Behandel je toch meer onderwerpen in je bericht, geef de onderwerpen dan een nummer.

Kom in de eerste alinea van je e-mailbericht meteen to-the-point. Wil je dat je collega de tweede versie van je concepttekst van commentaar voorziet, geef dat dan aan. Eventuele toelichting kun je daarna geven. Houd je bericht zo kort mogelijk, want het lezen van lange lappen tekst op een beeldscherm is niet prettig. Dreigt je e-mail toch erg lang te worden, voorzie je tekst dan van tussenkopjes.

Heb je dringend een reactie nodig, bel dan de ontvanger ook even om te zeggen dat je een e-mail hebt gestuurd. Je kunt zo de urgentie van je bericht nog eens benadrukken en de ontvanger kan aangeven of hij binnen de door jouw gestelde termijn kan reageren.

Overigens: gebruik voor de echte spoedgevallen niet de e-mail, maar pak de telefoon of loop even bij je collega langs.

Ga weloverwogen met bijlagen om

Met de bijlagenfunctie in je e-mailprogramma kun je bestanden met je e-mail meesturen. Hartstikke handig, alleen moet je ze wél daadwerkelijk toevoegen; het is weinig professioneel wanneer je in je e-mail naar een attachment verwijst dat ontbreekt. Je kunt dit voorkomen door er een gewoonte van te maken eerste de bijlage te selecteren en daarna pas het begeleidende bericht te schrijven. Schrijf altijd een begeleidende tekst bij een bijlage. Hierin leg je het doel van de bijlage uit en geef je precies aan wat je van de ontvanger verwacht.

Vraag je altijd af of het nodig is om de bijlage met je bericht mee te sturen. Staat de informatie al op het intranet of in een gedeelde map, dan is een link hiernaar voldoende. Zo voorkom je onnodig geheugengebruik in de mailbox van de ontvanger en overbelasting van het bedrijfsnetwerk. Bovendien hoeft de ontvanger minder handelingen te verrichten (bijlage openen, opslaan, verwijderen).

Wanneer je een bijlage meestuurt, let er dan op dat het bestand een duidelijke naam heeft en niet te groot is. Nietszeggende bestanden, zoals verslag.doc, en grote bestanden die niet snel geopend kunnen worden, wekken irritaties op bij de ontvanger. Nog erger is het wanneer je bijlage een virus blijkt te bevatten. Controleer bijlagen dan ook altijd op grootte en virussen.

Beperk het gebruik van cc

In sommige organisaties slibben inboxen helemaal dicht door de enorme hoeveelheid cc’tjes die worden verstuurd. Veelal heeft dit met de bedrijfscultuur te maken. Wees selectief in het versturen van zogenoemde cc'tjes. Gebruik cc alleen als het echt nodig is voor de ontvanger.

Let op correcte adressering

In de haast kan het wel eens gebeuren dat je een adres verkeerd intikt, de verkeerde contactpersoon in je adresboek selecteert of iemand vergeet. Controleer bij het verzenden van een bericht altijd of je het bericht aan de juiste perso(o)n(en) hebt geadresseerd. Vooral bij gevoelige informatie kan een dubbele check geen kwaad. Voorzie externe mail altijd van een disclaimer. In het geval een bericht bij de verkeerde persoon wordt bezorgd, zorgt deze ervoor dat derden hieraan geen rechten kunnen ontlenen of het bedrijf aansprakelijk kunnen stellen.

Let op formulering en spelling

Gaan we voor een brief nog eens goed zitten, bij het schrijven van een e-mail lijken goede omgangsvormen en spellingsregels te verdwijnen als sneeuw voor de zon: berichten vol spelfouten waarin alleen het hoognodige wordt vermeld. Hoewel zo niet bedoeld, kun je bij de ontvanger zo ongenuanceerd en kortaf overkomen.

Natuurlijk maakt het uit naar wie je de e-mail verstuurt - een snelle boodschap aan een collega kan informeler dan een bericht aan een klant - maar een correcte spelling en een goede formulering is ook een kwestie van fatsoen. Bovendien kom je met een goed geformuleerd en een juist gespelde tekst professioneler over dan met een rommelig bericht. Lees een e-mail dus goed door voor je hem verzendt en gebruik je spelling- en grammaticacontrole.

Wees ook voorzichtig met ironie, sarcasme en humor. Door het ontbreken van fysiek contact kan een grap gemakkelijk als kritiek worden uitgelegd.

2.3 Don’ts van emailen

Zet de ontvanger niet op het verkeerde been

Verstuur nooit een e-mail zonder het onderwerp in de onderwerpregel aan te geven. Verzend ook nooit een bericht zonder je naam te vermelden. Schrijf geen zinnen in hoofdletters. De ontvanger zal dit interpreteren als schreeuwen en zal denken dat je boos op hem bent.

Gebruik e-mail niet voor gevoelige onderwerpen of slecht nieuws

Hoewel e-mail in lastige situaties een aantrekkelijk alternatief lijkt, mag je je nooit achter een e-mail verschuilen. Door het ééndimensionale karakter van e-mail zie je niet hoe je bericht bij de ontvanger overkomt en kun je een misverstand niet meteen rechtzetten. Ook heb je geen idee van de omstandigheden en timing van het moment waarop je e-mail wordt gelezen. Hoe je slecht nieuws wel kunt brengen, leer je in de cursus Gesprekstechnieken.

Verzend geen vertrouwelijke informatie

In principe is e-mail niet geschikt voor het uitwisselen van vertrouwelijke informatie. Ook privé-informatie over collega’s wissel je niet uit via de mail. Een e-mail - of de reactie daarop – wordt nogal eens naar anderen doorgestuurd en dan komt je bericht terecht bij mensen voor wie jij hem niet had bestemd. Wees je ervan bewust dat in veel organisaties de systeembeheerder toegang heeft tot je e-mail.

Bcc

Wanneer je een bericht aan meerdere zakelijke contacten verstuurt, is het niet zo professioneel als de e-mailadressen van de geadresseerden voor iedereen zichtbaar zijn. Er zijn organisaties die maar al te gemakkelijk gebruikmaken van deze adressen om spam te versturen. Gebruik in een dergelijk geval bcc (blind carbon copy). De adressen die je hier invoert, zijn dan niet zichtbaar voor de anderen.

Wees niet te gemakzuchtig

Stuur niet voor ieder wissewasje een e-mail. Vraag je bij elk bericht even af of het wel verstandig is voor de betreffende boodschap e-mail als medium te gebruiken. Is een telefoontje of rechtstreeks contact met de collega, die een paar kamers verderop zit niet effectiever? En hoewel het een verleidelijk alternatief is om niet zelf de archiefkast in te hoeven duiken, is het niet verstandig om een e-mail te versturen waarin je om informatie vraagt die je zelf gemakkelijk kunt opzoeken. Het is niet collegiaal en zal voor de nodige irritaties kunnen zorgen.

Cc

Vele inboxen slibben dicht door de grote hoeveelheid cc’tjes die ‘voor de zekerheid’ en ‘ter info’ worden verstuurd. Doe hier niet aan mee en wees selectief in het versturen van cc’tjes.

To: alle afdelingen

In veel organisaties is het mogelijk om een bericht te versturen naar alle medewerkers of de medewerkers van een organisatieonderdeel, bijvoorbeeld de afdeling IT of Personeelszaken. Dat kan erg efficiënt zijn, bijvoorbeeld wanneer de directie een belangrijk bericht heeft.

Maar al te vaak wordt deze mogelijkheid uit gemakzucht gebruikt, omdat de verzender van de e-mail niet goed weet aan wie hij zijn bericht moet richten en voor het gemak de hele afdeling maar adresseert. Een bron van onnodige frustratie bij alle niet-terechte ontvangers.

Gebruik e-mail niet voor niet-zakelijke mail

Kettingbrieven horen niet thuis op het werk. Dat geldt ook voor e-mails die kwetsend kunnen zijn door grappen over huidskleur, afkomst, religie, seksuele geaardheid, ras of sekse. Gebruik je e-mail op het werk ook niet voor het verhandelen van spullen. De meeste organisaties hebben hier een speciaal hoekje voor ingericht op het intranet.

2.4 Checklist do's en don'ts

Do's	**Don'ts**
Let op formulering en spelling • Wees voorzichtig met ironie, sarcasme en humor • Voorkom spellingsfouten: lees je e-mail voor verzenden goed door en gebruik de spellingcontrole Wees helder en to the point • Zet in de onderwerpregel wat je van de ontvanger verwacht en wanneer • Begin je e-mail met je boodschap gevolgd door een toelichting • Behandel één onderwerp per e-mail • Behandel je meer onderwerpen per e-mail, nummer de onderwerpen dan • Houd je e-mail kort en zakelijk • Vraagt je e-mail echt snelle actie, bel dan de geadresseerde ook even op Ga weloverwogen met bijlagen om • Schrijf altijd een begeleidende tekst bij een bijlage: leg hierin uit wat het doel van de bijlage is en wat je van de ontvanger verwacht. • Vergeet de bijlage niet mee te sturen: leer jezelf aan eerst de bijlag te selecteren, daarna stel je de begeleidende mail op • Vraag je af of het noodzakelijk is om de bijlage toe te voegen of een alleen een link voldoende is • Voorzie de bijlage van een duidelijke naam • Controleer bijlagen altijd op grootte en virussen Beperk het gebruik van cc • Gebruik cc alleen als het echt nodig is voor de ontvanger. Let op correcte adressering • Controleer altijd of je je e-mail aan de juiste perso(o)n(en) adresseert • Voorzie externe e-mails altijd van een disclaimer	Zet de ontvanger niet op het verkeerde been • Verstuur nooit een e-mail zonder het onderwerp in de onderwerpregel aan te geven • Verzend ook nooit een e-mail zonder je naam te vermelden • Schrijf geen zinnen in hoofdletters • Verschuil je nooit achter een e-mail Verzend geen vertrouwelijke informatie • Verzend geen vertrouwelijke informatie of privé-informatie over collega's • Stuur e-mailadressen niet open en bloot mee als je een bericht verstuurt naar meerdere externe contacten Wees niet te gemakzuchtig • Stuur niet voor ieder wissewasje een e-mail • Vraag niet om informatie die je zelf gemakkelijk had kunnen opzoeken • Verstuur niet aan een hele afdeling een e-mail als je niet precies weet aan wie je je bericht moet richten • Ben niet gemakkelijk in het versturen van cc'tjes Gebruik e-mail niet voor niet-zakelijke mail • Doe niet mee aan kettingbrieven of ander 'grappen' • Gebruik je e-mail niet voor het verhandelen van spullen