TLP:CLEAR

Factsheet financiële fraude

Documentinformatie

Datum	8 februari 2024
Auteur(s)	Z-CERT
Versie	1.0

Z CERT
COMPUTER EMERGENCY RESPONSE TEAM VOOR DE ZORG

Inhoudsopgave

1. Inleiding

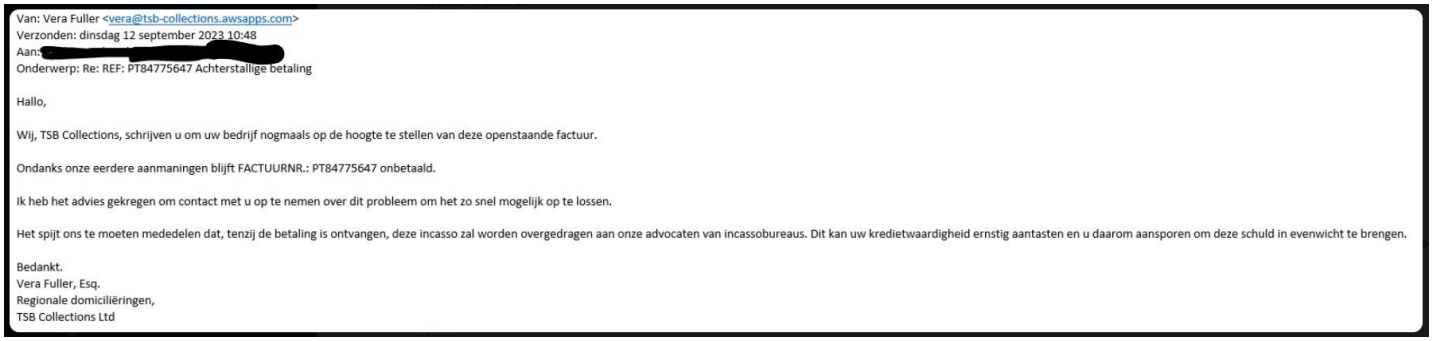
Eén van uw collega's ontvangt een e-mail of andersoortig bericht, zogenaamd van een directeur of manager, met daarin het urgente verzoek om met spoed een bepaald bedrag over te maken omdat er anders iets ergs gebeurt: een belangrijk contract gaat niet door, een boete wordt verhoogd of iets in die richting.

Bovenstaande is een algemeen voorbeeld van financiële fraude. In deze factsheet gaan we in op een paar varianten hiervan. Elk van de varianten kent gebruik van digitale middelen. Daarmee kiezen we dezelfde scope voor fraude als in ons jaarlijkse dreigingsbeeld. De hier behandelde voorbeelden zijn gericht op het veranderen van betalingen aan leveranciers en de salarisbetalingen aan medewerkers. Ook zogenaamde CEO fraude komt aan bod.
We gaan bij elke variant in op voorbeelden en best practices om hier mee om te gaan. De input hiervoor is afkomstig van deelnemers van Z-CERT. Elk hoofdstuk past op één bladzijde en is daarmee makkelijk te verspreiden onder uw collega's voor wie juist dat voorbeeld relevant is.

We hopen met dit document zorgaanbieders te helpen die voor het eerst aan de slag gaan om financiële fraude te voorkomen. Bent u al verder hiermee dan zijn de maatregelen waarschijnlijk al bekend of zelfs geïmplementeerd in uw organisatie. Stuur dan eens een goed lijkende nep-mail de organisatie in om te testen of uw collega's net zo goed handelen als u van ze verwacht!
Om in lijn te blijven met de volgende hoofdstukken, volgt ook voor deze inleiding een voorbeeld en een best practice.

1.1. Voorbeeld

Onderstaande mail is in het chatkanaal voor deelnemers van Z-CERT geplakt door een deelnemer om anderen te waarschuwen:



Van: Vera Fuller <vera@tsb-collections.awsapps.com>
Verzonden: dinsdag 12 september 2023 10:48
Aan: [redacted]
Onderwerp: Re: REF: PT84775647 Achterstallige betaling

Hallo,

Wij, TSB Collections, schrijven u om uw bedrijf nogmaals op de hoogte te stellen van deze openstaande factuur.

Ondanks onze eerdere aanmaningen blijft FACTUURNR.: PT84775647 onbetaald.

Ik heb het advies gekregen om contact met u op te nemen over dit probleem om het zo snel mogelijk op te lossen.

Het spijt ons te moeten mededelen dat, tenzij de betaling is ontvangen, deze incasso zal worden overgedragen aan onze advocaten van incassobureaus. Dit kan uw kredietwaardigheid ernstig aantasten en u daarom aansporen om deze schuld in evenwicht te brengen.

Bedankt.
Vera Fuller, Esq.
Regionale domiciliëringen,
TSB Collections Ltd

1.2. Best practice

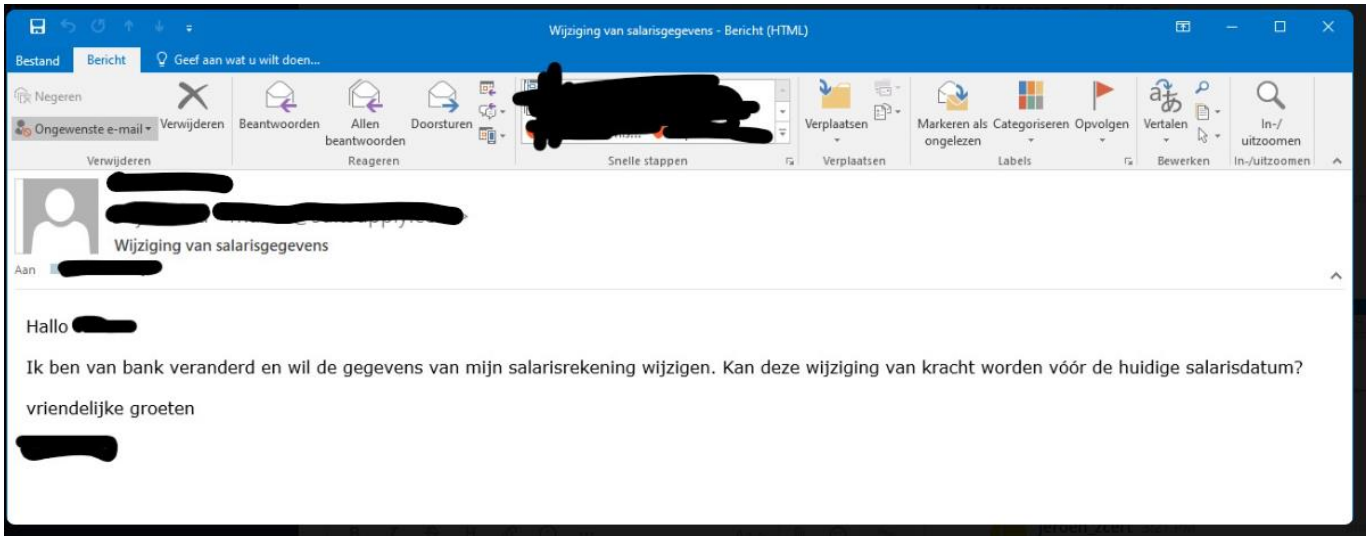
Leer collega's hoe een nepmail te herkennen. Bijvoorbeeld door gebruik te maken van tips en leermiddelen als deze:
https://www.digitaltrustcenter.nl/informatie-advies/phishing/hoe-herken-ik-een-phishing-e-mail
https://veiliginternetten.nl/maakhetzeniettemakkelijk/
https://www.digivaardigindezorg.nl/gehandicaptenzorg/home/informatiebeveiliging-privacy/onderwerp/phishing/

Zorg voor een eenvoudig proces waarmee collega's verdachte e-mails bij IT kunnen melden. Als er pieken zijn in de meldingen is dat aanleiding om extra aandacht te besteden aan dit onderwerp (waarschuwingen op een intranet, extra tips, voorbeelden delen enzovoort).

2. HRM en salaris

Iemand met een HR-functie krijgt een e-mail vanaf een (ogenschijnlijk) privé mailadres van een medewerker. Of met spoed het bankrekeningnummer voor salarisbetalingen en declaraties aangepast kan worden naar het meegestuurde nieuwe rekeningnummer.

2.1. Voorbeeld



Om dit soort voorbeelden echt te laten lijken is LinkedIn een goudmijn: het is heel makkelijk om medewerkers en HR medewerkers van dezelfde organisatie te vinden op LinkedIn. Ook het vinden van e-maildomeinen van zorgaanbieders is makkelijk en een nepmailadres maken dat lijkt op dat van de organisatie is daarmee zo gebeurd.

2.2. Best practice

Dit soort voorbeelden maakt duidelijk dat specifieke rollen in de organisatie getraind moeten worden op specifieke aspecten van security.

Veel zorginstellingen hebben een app of website waarmee personeel zelf wijzigingen kan doorvoeren in adres, bankrekening enzovoort. In die gevallen is de beste manier om fraude op dit vlak tegen te gaan om consequent te verwijzen naar de app en het de medewerkers zelf aan te laten passen. Doe dat *niet* in antwoord op de mogelijke nep-mail maar neem via de zakelijke gegevens per mail of telefonisch contact op.

Ook als uw organisatie niet een dergelijke app gebruikt, is het veilig om naar het standaard proces voor bankrekeningnummers aanpassen te verwijzen. Dit zal dan via een vast mailadres, een servicedesk of vergelijkbaar georganiseerd zijn en met vaste controlepunten in het proces voordat de wijziging wordt doorgevoerd.

3. Inkoop en crediteurenadministratie

Een kwaadwillende maakt een mooie factuur, plakt er een logo op van een leverancier, vermeldt zijn bankrekening en stuurt deze naar een grote groep bedrijven, al dan niet in de zorg. Er trapt altijd wel iemand in. Zorg dat u het niet bent!

3.1. Voorbeeld

Voorbeeld 1

Vanaf een nep e-mailadres wordt een factuur gestuurd die zogenaamd van een leverancier is. Dit kan een bekende leverancier zijn of een onbekende.

Voorbeeld 2

Bij de leverancier is ingebroken in de e-mail omgeving waardoor van echte e-mailadressen nepfacturen binnenkomen. Of een "op de domeinnaam van de leverancier" lijkende domeinnaam wordt geregistreerd en vandaar worden nepfacturen gestuurd.

Voorbeeld 3

Een kwaadwillende heeft zich bij een grote leverancier voorgedaan als organisatie met het verzoek om facturen voortaan naar een ander (goed gelijkend)adres te mailen. Vanaf weer een ander mailadres, dat juist lijkt op dat van de leverancier overtuigt dezelfde kwaadwillende u ervan dat u voortaan de facturen van de leverancier van af een nieuw mailadres zult ontvangen en dat de bankrekening is veranderd.

De kwaadwillende onderschept zo echte facturen, soms met echte prestatieverklaring als bijlage, voorzien van echte namen, projectnummers, inkoopordernummers enzovoort. Men kan deze goed namaken en doorsturen, voorzien van het nieuwe bankrekeningnummer.

3.2. Best practice

Voor deze voorbeelden is beveiligingsbewustzijn nodig bij de medewerkers die dergelijke e-mail kunnen ontvangen. De nep-mail komt immers van een legitieme afzender. Zie hiervoor de tips in het inleidende hoofdstuk. Als de mail van een onbekende leverancier komt, voorkomt een strak proces voor het aanmaken van de gegevens mogelijke ellende: wie is de ‘eigenaar’ van de leverancier in uw organisatie, klopt de factuur en kloppen de gegevens van de leverancier? Zeker bij een eerste betaling extra belangrijk om te controleren.

Voor het tweede en derde voorbeeld is het belangrijk om pas bankrekeningen van leveranciers aan te passen nadat gecontroleerd is of de aanpassing klopt. Implementeer hiervoor een procedure waarbij u op een *andere* manier contact zoekt met de leverancier dan de manier waarop het nieuwe bankrekening is doorgegeven. In de praktijk komen (zogenaamde) wijzigingen van bankrekening vooral per e-mail of post binnen. Dan is bellen ter controle een goede maatregel. Gebruik een reeds bekend nummer en niet een eventueel tegelijkertijd met het bankrekening veranderde telefoonnummer….

4. CEO fraude

Een directeur, lid van de Raad van Bestuur of ander hooggeplaatste functionaris meldt zich bij iemand die op de administratie werkt met een spoedverzoek; zij wil bijvoorbeeld een spoedbetaling uit laten voeren, een groot aantal (digitale)cadeaubonnen hebben om aan relaties te geven of iets in die richting. Gehoorzaam je zonder meer 'de baas', of blijf je kritisch?

4.1. Voorbeeld

body:
Hallo Simone,

Heb je een momentje? Ik zou graag je aandacht willen voor een kleine taak, antwoord op mijn e-mail met je persoonlijke mobiele nummer, zodat ik je kan sms'en wat ik wil dat je doet.

Groeten

<directeur>
Managing Director
Ziekenhuis[redacted]

Verzonden vanaf mijn mobiel *Edited*

4.2. Best practice

Bij deze vorm van financiële fraude voelen medewerkers zich vaak onder druk gezet.

- De direct leidinggevende of een hoger geplaatste collega vraagt iets,
- er is kennelijk haast bij en
- vaak volgen steeds dwingender herinneringen als het niet snel genoeg wordt opgevolgd.

Leer de personen in rollen die dit soort berichten ontvangen (administratie) hoe de berichten te herkennen zijn. Maak ook duidelijk dat sms en whatsapp geen spamfilters hebben.
Leer de personen namens wie dit soort berichten vaak verstuurd worden (directie) dat ze alleen vanaf hun zakelijke mail of telefoonnummer communiceren. Dan is het voor de ontvangers makkelijker om echt van nep te onderscheiden.

5. Checklist – weerbaarheid tegen financiële fraude

(waar 'mail' staat kun je ook lezen 'chatberichten', 'telefoontjes' enz.)

Proces: personeelsadministratie	✓	✗
Het wijzigen van bankrekeningnummers van medewerkers verloopt volgens een vast proces.		
In dit proces zijn controlepunten ingebouwd om fraude/fouten te voorkomen. Bijvoorbeeld: checkvraag bij medewerker, ontvangstbevestiging naar medewerker, 4 ogen principe.		
Medewerkers kunnen zelf hun bankrekeningnummer wijzigen in het systeem, bijvoorbeeld via een app.		
Iedereen met rechten om bankrekeningnummers te wijzigen is getraind in het herkennen van nepmails.		
Wij oefenen gericht om te toetsen of medewerkers nepmails herkennen en werken volgens de afgesproken processen.		
Proces: crediteurenadministratie	✓	✗
Het wijzigen van bankrekeningnummers van leveranciers verloopt volgens een vast proces.		
In dit proces zijn controlepunten ingebouwd om fraude/fouten te voorkomen. Bijvoorbeeld: checkvraag bij leverancier, ontvangstbevestiging naar leverancier, 4 ogen principe.		
Wij betalen facturen niet als deze een ander bankrekeningnummer vermeldt dan bij ons bekend is.		
Bij betalingen aan zogenaamde 'eenmalige crediteuren' voeren wij controles uit op het bankrekeningnummer.		
Iedereen met rechten om bankrekeningnummers te wijzigen is getraind in het herkennen van nepmails.		
Wij oefenen gericht om te toetsen of medewerkers nepmails herkennen en werken volgens de afgesproken processen.		
Proces: creditcardbetalingen/uitgifte cadeaubonnen	✓	✗
Aanvragen voor VVV-bonnen of andere cadeaubonnen lopen via een vast proces of via een speciaal daarvoor bestemd systeem.		
In dit proces zijn controlepunten ingebouwd om fraude/fouten te voorkomen. Bijvoorbeeld: checkvraag bij aanvrager, ontvangstbevestiging naar aanvrager, 4 ogen principe.		
Iedereen die werkt in deze processen is getraind in het herkennen van nepmails.		
Wij oefenen gericht om te toetsen of medewerkers nepmails herkennen en werken volgens de afgesproken processen.		
Bestuur/directie/hoger management gebruikt de vaste processen, zonder uitzonderingen. (dan weten de uitvoerenden in het proces makkelijker dat een aanvraag nep is)		
IT/ServiceDesk/Security	✓	✗
Er is een eenvoudig proces om nepmails te melden bij de ServiceDesk		
Medewerkers kennen en gebruiken dit proces.		
DMARC is geïmplementeerd voor al onze mail-domeinen		