Enkele facetten van identiteitsdiefstal

Bijdrage aan de studieavond van 16.10.2014
georganiseerd door ARSON

Inhoudstafel

- **Strafbepalingen**
- Enkele W-vragen
- Nieuwe technologieën
- Voorbeelden identiteitsfraude
- Enkele tips en tricks

Definitie: wettelijke omschrijving

Art. 231 Strafwetboek: Hij die **in het openbaar een naam aanneemt, die hem niet toekomt**, wordt gestraft met een gevangenisstraf van 8 dagen tot 3 maanden en met een geldboete van 25 frank tot 300 frank, of met één van deze straffen alleen.

(Algemeen opzet volstaat)

(Openbaar = bv. Hotelregister maar niet prive-onderhoud)

Art 196 Strafwetboek: Met opsluiting van 5 tot 10 jaar worden gestraft de andere personen (niet ambtenaren) die **in authentieke en openbare geschriften valsheden plegen** …

- Valse handtekeningen
- Namaking of vervalsing van handtekeningen en geschriften
- Overeenkomsten, beschikkingen, verbintenissen of schuldbevrijdingen valselijk op te maken …
- Toevoeging of vervalsing van bedingen, verklaringen of feiten die deze akten ten doel hadden op te nemen of vast te stellen.

(Ook private geschriften – Bijzonder opzet vereist)

Art 197 Strafwetboek: … hij die **gebruik maakt van de valse akte of het valse stuk**, wordt gestraft alsof hij de dader van de valsheid was.

(gebruik duurt zolang nuttig uitwerksel volbrengt)

Inhoudstafel

- Strafbepalingen
- **Enkele W-vragen**
- Nieuwe technologieën
- Voorbeelden identiteitsfraude
- Enkele tips en tricks

Definitie: Wat is identiteit?

- Samengaan van meerdere aspecten zoals:
  - Naam
  - Adres
  - PIN-code
  - Vingerafdrukken
  - Andere aspecten

Wat is identificatie?

- Som van
  - Kennen (vb. PIN-code)
  - Hebben (vb. documenten, kaarten)
  - Zijn (vb. foto, vingerafdruk)

… op weg naar meer …

- Geen doel op zich
- Middel tot het bekomen van navolgend voordeel

Waarom?

- Verrichten van aankopen
- Controle verwerven over accounts
- Openen rechten
  - Misbruik sociale zekerheid
  - Ontvangen uitbetalingen verzekeringen
- Zich 'verstoppen'
  - Opgeven van valse identiteit bij controle om link met zwaardere feiten te verbergen
- Andere criminele contexten

Welke omvang?

- Arrondissement Brussel (laatste 6 maanden – indicatief!)
  - Usurperen naam: 366 feiten
  - Valsheid en gebruik: 50 feiten
- Dark number
  - Aangiftebereidheid slachtoffers
  - Aangifteberidheid (private) organisaties
- Schade
  - Financiëel
  - Imago

Waar?

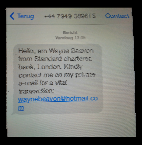
- Volledige fantasie
- Diefstal echte documenten
- Kennisname via open bronnen
  - Internet
  - Staatsblad
- Aankopen
  - Dumps van gehackte databanken

Inhoudstafel

- Definities
- Enkele W-vragen
- **Nieuwe technologieën**
- Voorbeelden identiteitsfraude
- Enkele tips en tricks

Nieuwe technologieën

- Opportuniteiten criminelen:
  - Malware
    - (droppen van een virus)
  - Phishing
    - (afleiden naar een website)
  - SMiShing
    - (inkomende boodschappen via SMS)
  - Spear phishing
    - (zich voordoen als collega om paswoorden te verkrijgen)
  - Vishing
    - (afleiden naar een telefoonnummer)



Nieuwe technologieën

- Verhoogde risicograad
  - Afhankelijkheid van digitale info ipv face to face
  - Massa info in één databank: risico op massa-diefstal
  - Nieuwe wijze van contacten tussen criminelen en potentiële slachtoffers (vb. phishing)
  - Snelle verspreiding nieuwe MO via het internet.
  - Internet = bron van identiteitsgegevens

Inhoudstafel

- Strafbepalingen
- Enkele W-vragen
- Nieuwe technologieën
- **Voorbeelden van identiteitsfraude**
- Enkele tips en tricks

Voorbeelden gebruik identiteitsfraude

- Social engineering
- Post-it fraude
- Spam mailings
- Frauduleuze bestellingen
- Phishing en aanverwanten
- Bankkaartfraude

Social engineering

= Het zich voordoen als een verantwoordelijke van een grote firma teneinde financiële transacties te laten plaatsvinden

= CEO fraude

Social engineering

Contactname financiële instelling

- Via telefoon
- Via e-mail (adres sterk gelijkend op het echte adres met gebruik van naar van de zogezegde verzender)

Social engineering

- Belangrijk voor het onderzoek:
  - Gebruikte telefoonnummers
  - Gebruikte e-mailadressen – Full headers
  - Details begunstigde bankrekeningen
  - Snelle info = snelle tussenkomst

Social engineering

- Vaststellingen in het onderzoek
  - Internationale bankverrichtingen
  - Eerste overschrijvingen vaak naar oost-Europa
  - Verdere witwas in verre oosten (Hong-Kong)
  - Basis fraude in Israël

Post-it fraude

= het stelen van poststukken, gevolgd door het aanpassen van essentiële betalingsgegevens

Post-it fraude

- Belangrijk voor het onderzoek:
  - Gebruikte telefoonnummers
  - Gebruikte e-mailadressen – Full headers
  - Details begunstigde bankrekeningen
  - Snelle info = snelle tussenkomst
- Vaststellingen in het onderzoek
  - Verdachten uit het Afrikaanse milieu

Spam mailings

= Het verzenden van poststukken of e-mails met een factuur, in naam van een onwetende vennootschap.

Aanschrijven van 'grote' bedrijven voor 'kleine' bedragen

Frauduleuze bestellingen

= het plaatsen van allerhande bestellingen op naam van een nietsvermoedende vennootschap of natuurlijke persoon.

Frauduleuze bestellingen

- Gebruik maken van de 'identiteitsgegevens' van een vennootschap
- Informatie uit open bronnen zoals het Staatsblad of via boekhouder
- Bestellingen van snel verhandelbare goederen of op vraag van kopers
- Heb aandacht voor details door 'klant' aangeleverde informatie

Frauduleuze bestelingen

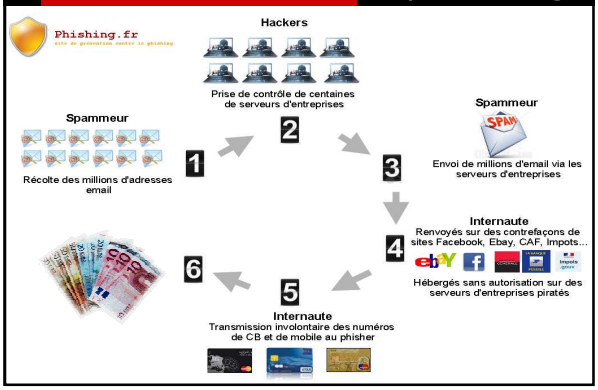
1. Bestelling via internet/fax …
2. Mail naar fraudeur met voorstel
3. Mail terug met akkoord, stempel en betalingsbewijs
4. Aanvaarden bestelling en levering
5. Afleiden levering op het laatste moment naar nieuwe locatie

Fraude bankrekeningen

- **Phishing**
  = het 'vissen' via e-mail naar bancaire informatie:
  - Verzamelen van toegangscodes
  - Verzamelen van kredietkaartgegevens

- **Pharming**
  = het aanwenden van 'gephishte' inlichtingen

Verloop Phishing



Phishing - bron

Opmerkelijk:

- 'Redactionele kwaliteit' van de e-mail → Google translator?
- Hyperlinks die verwijzen naar het buitenland of naar sites http://XXXXXX.bank.XXX
- Webpagina die vastloopt
- Navolgend telefonisch contact

Phishing - bron

De : BNP Paribas Fortis België
Date : 24/04/2013 12:54:11
A : undisclosed-recipients:;
Sujet : BNP Paribas Fortis Alert - Uw Internet Bankieren op slot

Geachte klant,

Onlangs heeft onze gegevens blijkt dat uw BNP Paribas Fortis rekening mogelijk gemaakt door een derde partij illegale binnenkomst.

De veiligheid van uw account is onze primaire zorg, daarom besloten om toegang tot uw account tijdelijk te beperken. Om volledige toegang tot uw account moet u uw gegevens te herstellen om te bevestigen via de link: **Klik hier**

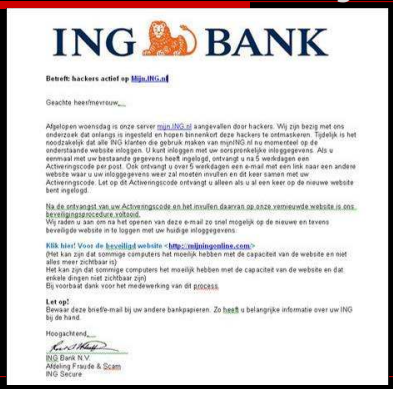
Zodra uw gegevens door ons zijn gecontroleerd en bevestigd, word er zo spoedig mogelijk contact met u opgenomen door een van onze medewerkers om de toegang tot uw account volledig te herstellen .

Wij danken u voor uw medewerking.

Met vriendelijke groet,
BNP Paribas Fortis België.

http://bhounderhijk.co/bnpparibasfortis.logonto.pc.html/
Opzoekingen 'Whois'
Website geregistreerd op 24.04.2013 (= datum van verzending bericht)
door Olivier Giroud uit Parijs
e-mail registratie 'beautifulflower510@yahoo.com'

Phishing - bron



ING BANK

Betreft: hackers actief op Mijn.ING.nl

Geachte heer/mevrouw,...

Afgelopen woensdag is onze server mijn.ING.nl aangevallen door hackers. Wij zijn bezig met ons onderzoek dat onlangs is ingesteld en hopen binnenkort deze hackers te ontmaskeren. Tijdelijk is het noodzakelijk dat alle ING klanten die gebruik maken van mijnING.nl nu momenteel op de onderstaande website inloggen. U kunt inloggen met uw eerspronkelijke inloggegevens. Als u eenmaal met uw bestaande gegevens heeft ingelogd, ontvangt u na 5 werkdagen een Activeringscode per post. Ook ontvangt u over 5 werkdagen een e-mail met een link naar een andere website waar u uw inloggegevens weer zal moeten invullen en dit keer samen met uw Activeringscode. Let op dit Activeringscode ontvangt u alleen als u al een keer op de nieuwe website bent ingelogd.

Na de ontvangst van uw Activeringscode en het invullen daarvan op onze vernieuwde website is ons beveiligingsprocedure voltooid.
Wij raden u aan om na het openen van deze e-mail zo snel mogelijk op de nieuwe en tevens beveiligde website in te loggen met uw huidige inloggegevens.

Klik hier! Voor de beveiligd website <http://mijningonline.com>
(Het kan zijn dat sommige computers het moeilijk hebben met de capaciteit van de website en niet alles meer zichtbaar is)
Het kan zijn dat sommige computers het moeilijk hebben met de capaciteit van de website en dat enkele dingen niet zichtbaar zijn)
Bij voorbaat dank voor het medewerking van dit process.

Let op!
Bewaar deze briefe-mail bij uw andere bankpapieren. Zo heeft u belangrijke informatie over uw ING bij de hand.

Hoogachtend,...

ING Bank N.V.
Afdeling Fraude & Scam
ING Secure

Pharming: Gephishte toegangscodes

- Doel 1: **controle verwerven** over de rekening van het slachtoffer
- Doel 2: **rekening** slachtoffer **debiteren** ten gunste van Money Mule
- Doel 3: rekening Money Mule **omzetten in cash**

Pharming: Kredietkaartgegevens

- Doel: gebruik kredietkaartgegevens voor non face-to-face aankopen
  - Bestellingen via het internet
  - Bestelling per telefoon

Bankkaartfraude

- Nagemaakte bankkaarten
- Shoulder surfing
- Skimming of shimming

Bankkaartfraude: counterfeit

= het gebruiken van gekopieerde bankkaartgegevens die aangebracht zijn op 'toonbare' dragers

- Bron data voornamelijk hackings van grote databases
- Identiteitsfraude op het moment van de hacking
- Identiteitsfraude op het moment van het aanbieden van de bankkaarten

Bankkaartfraude: shoulder surfing

= het over de schouder van het slachtoffer meekijken teneinde de geheime PIN-code te bekijken, gevolgd door de diefstal van de bankkaart

- Identiteitsfraude op het moment van het gebruik van de gestolen bankkaart (PIN-code)

Bankaartfraude:skimming - shimming

= Het kopiëren van de bankkaartgegevens van de magnetische strip die zich op achterkant van bankkaarten bevindt (van de chip) + het bekomen van de bijhorende PIN-code

- Identiteitsfraude op het moment van het gebruik van de gekopieerde bankkaart (PIN-code)

Inhoudstafel

- Strafbepalingen
- Enkele W-vragen
- Nieuwe technologieën
- Voorbeelden identiteitsfraude
- **Enkele tips en tricks**

Aandachtspunten

- Vingerafdrukken + DNA vervalste documenten
- Vernietig originele documenten niet!
- Full headers e-mailverkeer (I.P.-adressen)
- Gebruikte telefoonnummers en e-mailadressen

Aandachtspunten

- Opzoekingen via het internet op sleutelwoorden zoals naam, telefoonnummer, rekeningnummer, …
- Is het posttraject van de vervalste stukken te reconstrueren?
- Kan er met een dubbele bevestiging gewerkt worden (bv. post en e-mail)?

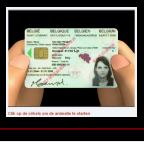
www.checkdoc.be

Initiatief van FOD Binnenlandse Zaken

- Gestolen
- Verloren
- Verlopen
- Ongeldig
- Niet uitgereikt

CHECKDOC

BEVEILIGINGSELEMENTEN VAN DOCUMENTEN



DOC STOP 00800 2123 2123 +32 2 518 2123

Raadgevingen
Canadese Consumer Measures Committee

- Houd de ICT up to date (fire walls, paswoorden, encryptie, …)
- Blijf bewust van wat je verzameld: niet nodig = niet verzamelen
- Geef de klanten de nodige privacy bij contacten met uw organisatie (vb loketten)
- Geef niet iedereen toegang tot alle informatie (need to know ≠ nice to know)
- Weet met wie u praat (contact organisatie – klant)
- Beter op netwerk dan op lokale harde schijf (veiligheidsupdates, verlies pc, vernietiging pc einde carrière)
- Verwittig de systeembeheerder bij 'eigenaardigheden' van databanken of netwerken
- Terug naar huis = clean desk