

Phishing 4 **Bad Sushi**

Ferdinand Vroom

Agenda

1. Phishing
2. Quizzzzzz
3. Maatregelen
4. Phishing 4 Phishers
5. Conclusies
6. Vragen

De [Postbank](#) gevist...

Phishing

Wat is Phishing?

Phishing is een vorm van **oplichting**.

Criminelen gebruiken internet om via phishing **persoonlijke informatie** van derden in hun bezit te krijgen.

Ze **misleiden** met **e-mails** en **websites** die uitingen lijken van bekende en betrouwbare organisaties. Maar in werkelijkheid zijn het vervalsingen.

In die e-mails en op die websites vragen ze naar **logingegevens**, **creditcardinformatie** en/of **sofi-nummer**.

Phishing

Gevoelige informatie:

Inlog gegevens

Creditcard nummers

Sofinnummers

Systeem Specifieke Credentials (Cookies, TAN)

Doel: Stelen van identiteit

Phishing

Wie:

Criminele netwerken (Russian Business Network)

Waarvoor:

Witwassen van geld

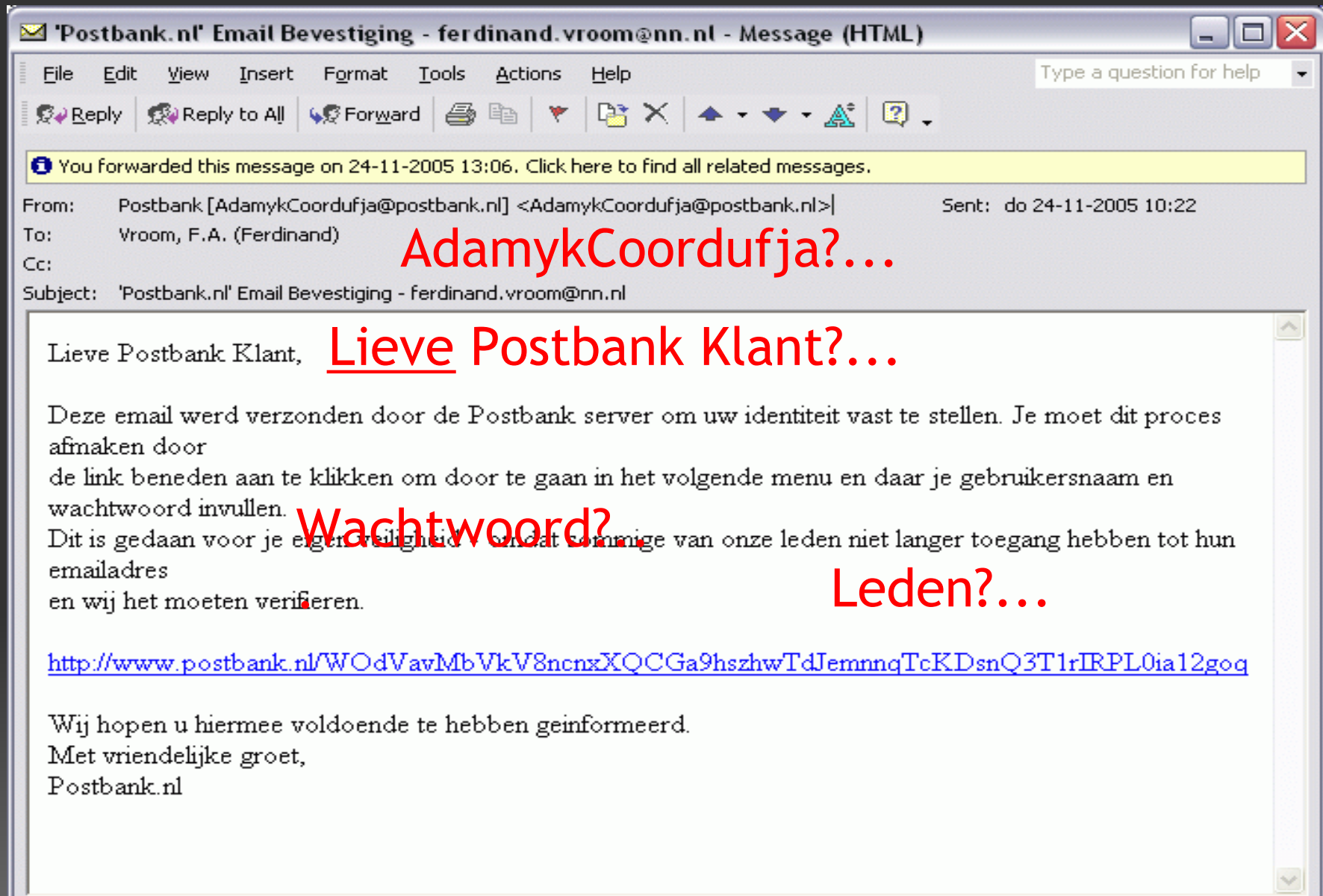
Phishing

- Email
 - Instant Messaging
 - Malware
 - Code Injection
-
- Spear Phishing
 - Vishing (VOIP)
 - Pharming (DNS)

Quizzzzzz



Quizzzzzz



Quizzzzzz

Waar op te letten:

- Beveiligingsinformatie of Persoonlijke informatie
- Haast
- Personalisering
- Rekeningnummer
- Huisstijl
- Taal
- Telefoonnummer
- Beveiliging SSL
- Link

Maatregelen

1. Klant Bewustzijn d.m.v. Gedraglijn
2. Detectie en Data Beveiliging Gedraglijn
3. Web Applicatie
4. Incident Respons
5. Online Communicatie Gedraglijn
6. Gedraglijn voor Algemene Voorwaarden

Maatregelen

Klant Bewustzijn verhogen door te informeren

- Beveiligingsrisico's beschrijven
- Maatregelen toelichten
- Standaard communicatie
- Persoonlijke Beveiliging
- PC beveiliging

Maatregelen

Detectie om het "window of opportunity" te verkorten

Domein Namen (google.com, ingdirect.com)

Monitoring

- DNS (A, CNAME, NS en MX)
- WHOIS
- SSL Certificaten
- WWW

Maatregelen

Merk Misbruik

Logo

Risico

Shutdown (Service)

Maatregelen

Email Detectie

SPAM Karakteristieken

- Spoofed Emailadres
- Grote Hoeveelheden met Identieke Inhoud
- Dubieuze Kwaliteit

Maatregelen

Email Monitoring

Bij Produkt van Anti- Spam Produkten

Email Filtering

Signature

Catch All Mailbox Monitoring

Money Mule Recruiting

Nep Accounts

Maatregelen

WWW

Nieuwsgroepen

Blogs

Alert Service

Maatregelen

Front Office Monitoring

Referrer
Geolocatie

Simultaan login met verschillende IP adressen

Mislukte logins %

Navigatie Patroon

Maatregelen

Back Office Monitoring

Statistische Afwijkingen

Verdachte Bestemmingen

Maatregelen

Meldingen van Klanten

Call Centre

Instructies op de Website

Dedicated Emailadres

SMS Alert

Maatregelen

Logging!...

Maatregelen

Forensische Analyse

Analyse van Fake Websites

Trojan Analyse

Preventieve Analyse (tussen banken)

Maatregelen

Web Applicatie

Afbeeldingen

- Naam wijzigen, oude bewaren
- SessionID in de naam van de afbeelding

Waarschuwingpagina

Host en Link Conventie

<http://secure.postbank.nl>

Conclusies

Phishing is een vorm van **Social Engineering**
Dus bewustzijn is erg belangrijk!

Diefstal van identiteit

Detectie vermindert de schade

Alle data moet beveiligd worden voor analyse
Continue verbeteren

Phishing 4 Phishers

Forensisch onderzoek:

Phishing agenten

niet de technische methoden

Doel: Server shutdown

Fraude audits = post hoc

Phoney Tokens = pro actief

Phishing 4 Phishers

Methode:

Phishers databases vullen met **gemarkeerde credentials**

Lokken van Phishers naar **namaak systemen**

Profielen maken van **gedrag** van Phishers

Denk aan serienummers van bankbiljetten

Phoneytokens (Phishing Honey Tokens)

Phishing 4 Phishers

Phoney Tokens

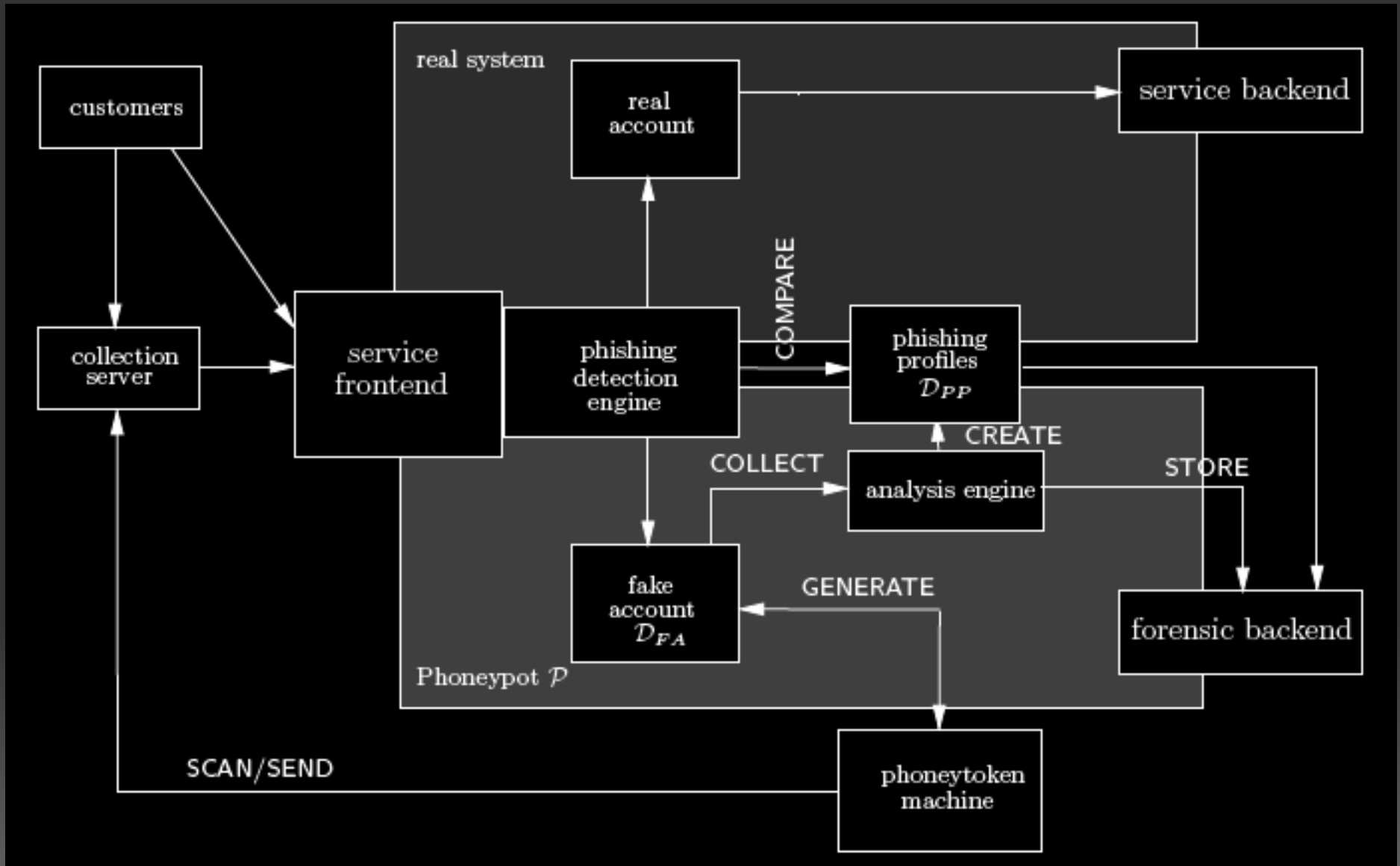
Alfanumeriek: random, woordenboeken, publieke lijsten

Numeriek: sequentie verbergen, datum, tijd

Functie met **sleutel** om authenticiteit van Phoney Token vast te stellen

Phisher kan geen Phoney Token maken!

Phishing 4 Phishers



Phishing 4 Phishers

Phoneypot

Eerlijke gebruiker -> echte systeem

Phisher -> Phoneypot

Mogelijke Phisher, afhankelijk van overeenkomsten:

- Phoneypot
- Transactie uistellen

Phishing 4 Phishers

Analyse

Log bestanden

Typisch gedrag van een echte gebruiker

Verschillende netwerken

Forensische standaards

Phishing 4 Phishers

Analyse

Passief afnemen van "vingerafdrukken"

ISO/ OSI 3 en 4:

Adressen, Geografische lokatie

Buitenland/ vaste lokatie

Vertragingen

Proxies, Botnets

Phishing 4 Phishers

Analyse

Passief afnemen van "vingerafdrukken"

ISO/ OSI 7:

Browser/ OS/ HTTP headers

DNS requests

Afbeeldingen, CSS, JS

Volgorde en timing

Vragen



info@ferdinandvroom.nl

Links

Anti Phishing Work Group

<http://www.antiphishing.org/>

Carnegie Mellon Phishing Game

http://cups.cs.cmu.edu/antiphishing_phil/new/index.html

OWASP Netherlands

<http://www.owasp.org/index.php/Netherlands>