

exact
Live
2019

Hoe houdt Exact zijn systemen veilig?

Jack Krul & Bastiaan van der Vis

=exact



Agenda:

- 1) Introductie
- 2) Dreigingslandschap
- 3) Belangrijkste risico's / Voorbeelden
- 4) Vragen / afsluiting

exact
Live
2019

Introductie

Jack Krul



Bastiaan van der Vis



Wat is informatiebeveiliging

“**Informatiebeveiliging** is het geheel van preventieve, detectieve, repressieve en correctieve maatregelen alsmede procedures en processen die de beschikbaarheid, exclusiviteit en integriteit van alle vormen van informatie binnen een organisatie of een maatschappij garanderen, met als doel de continuïteit van de informatie en de informatievoorziening te waarborgen en de eventuele gevolgen van beveiligingsincidenten tot een acceptabel, vooraf bepaald niveau te beperken.”

Met andere woorden.....

Met maatregelen de kans op negatieve impact op de beschikbaarheid, integriteit of vertrouwelijkheid zou klein mogelijk houden.

Hoe doet Exact dat....



Actoren en hun motieven



Klanten /
Medewerkers /
Partners



Interne



Script
Kiddies



Criminelen



Hacktivisten



Staten

MOTIVES

Onbewust

Wraak
Financieel

Plezier
Onwetend-
heid

Financieel
Spionage

Ideologisch

Financieel
Ideologisch



Wat zijn de mogelijke dreigingen voor Exact

	Overheid	Vitaal	Privaat	Burgers
Staten/ staatsgelieerd	Spionage Informatiemanipulatie	Sabotage Verstoring Spionage	Spionage Systeemmanipulatie	Spionage
Criminelen	Verstoring Systeemmanipulatie Informatiediefstal	Verstoring Systeemmanipulatie	Verstoring Informatiemanipulatie Informatiediefstal Systeemmanipulatie	Verstoring Informatiemanipulatie Informatiediefstal Systeemmanipulatie
Terroristen	Sabotage	Sabotage		
Hacktivisten	Verstoring	Verstoring	Verstoring Informatiemanipulatie	
Cybervandalen en scriptkiddies	Verstoring	Verstoring	Verstoring	
Insiders	Informatiediefstal		Informatiediefstal	
Niet opzettelijk handelen	Storing/uitval Lek	Storing/uitval Lek	Storing/uitval Lek	Lek

Bron: NCSC / CSBN2019



exact
Live
2019

Maar wat is uw data eigenlijk waard?



NETFLIX

= exact

Email Account For Sale (Email + Password)

YAHOO!
Gmail
by Google

\$1

ADD TO CART

Ecommerce Accounts (Name + Password)

ebay
PayPal
amazon

\$1-
\$80

(price depends on balance)

ADD TO CART

Service Apps (Name + Password)



UBER

NETFLIX

\$2

ADD TO CART

Social Security Number



\$1

ADD TO CART



exact
Live
2019

Maar wat is uw data eigenlijk waard?

HOME SALES MESSAGES ORDERS LISTINGS BALANCE FEEDBACK FORUMS API SUPPORT

Fraud Accounts & Bank Drops Uber ★★★UNLIMITED FREE UBER RIDES 2017★★★

LISTING OPTIONS

Contact Seller
Favorite Listing
Favorite Seller
Alert when restock
Report Listing

BROWSE CATEGORIES

- Fraud 48144
- Drugs & Chemicals 260131
- Guides & Tutorials 16835
- Counterfeit Items 10118
- Digital Products 18955
- Jewels & Gold 1895
- Weapons 5590
- Carded Items 4006
- Services 8213
- Other Listings 4389
- Software & Malware 3672
- Security & Hosting 914

UBER

★★★UNLIMITED FREE UBER RIDES 2017★★★

- Get Unlimited Uber Rides for Free! - you can repeat this 100000 times

Sold by Kanagakim - 610 sold since Dec 23, 2016 Vendor Level 1 Trust Level 4
318 items available for auto-dispatch

Product class	Features	Origin country	Features
Quantity left	Digital goods	Ships to	Worldwide
Ends in	Unlimited	Payment	Worldwide Escrow
	Never		

Default - 1 days - USD +0.00 / item

Purchase price: USD 0.99

Qty: 1 Buy Now Buy Now

Buy Now Queue

0.0004 BTC / 0.0235 XMR / 0.0037 ETH / 0.9900 ZEC /

Description Bids Feedback Refund Policy

Listing Feedback

Buyer	Date	Time	Comment
G**6	March 1, 2017	11:11	Late response but great servi
s**4	January 26, 2017	03:57	A+

200 Million Hacked YAHOO! Accounts Up On SALE



Yahoo 200M

By peace_of_mind (100.0%) Level 1 (14)

0 3.0000 / BTC 3.0000

In stock.

Postage Option

Escrow Yes, escrow by RealDeal is available.

Class Digital

Ships From Worldwide

Qty: 0

Buy It Now

Favorite Question

1. (CXO) Fraude / via email

From: Antonius Shlyakhter <ashlyakhter@inbox.ru>
Sent: maandag 14 januari 2019 13:26
To: ashlyakhter@inbox.ru
Subject: st :0285 - f kes

I am aware f es one of your passwords. Lets get right to the purpose. Not a single person has compensated me to investigate you. You do not know me and you are most likely thinking why you are getting this email?

in fact, i actually setup a malware on the adult videos (pornography) web-site and there's more, you visited this web site to have fun (you know what i mean). When you were watching video clips, your browser began working as a Remote Desktop with a key logger which provided me with access to your display screen and webcam. Right after that, my software program gathered all your contacts from your Messenger, social networks, and e-mail . Next i made a double video. 1st part shows the video you were watching (you've got a nice taste lmao), and 2nd part shows the recording of your web camera, yea it is u.

You actually have 2 alternatives. Shall we read these choices in particulars:

Very first option is to dismiss this email. in this instance, i will send your actual recorded material to each one of your contacts and thus just think regarding the awkwardness you experience. and as a consequ ence should you be in an important relationship, just how it will certainly affect?

Another option should be to compensate me 100 000 . Let us refer to it as donation . Consequently, i must contact you will send delete your video footage . You will have extra money in your life like this money

urgent payment



Phill Robinson <dyrektor@naver.com>

Aan

Vervalt 22-Sep



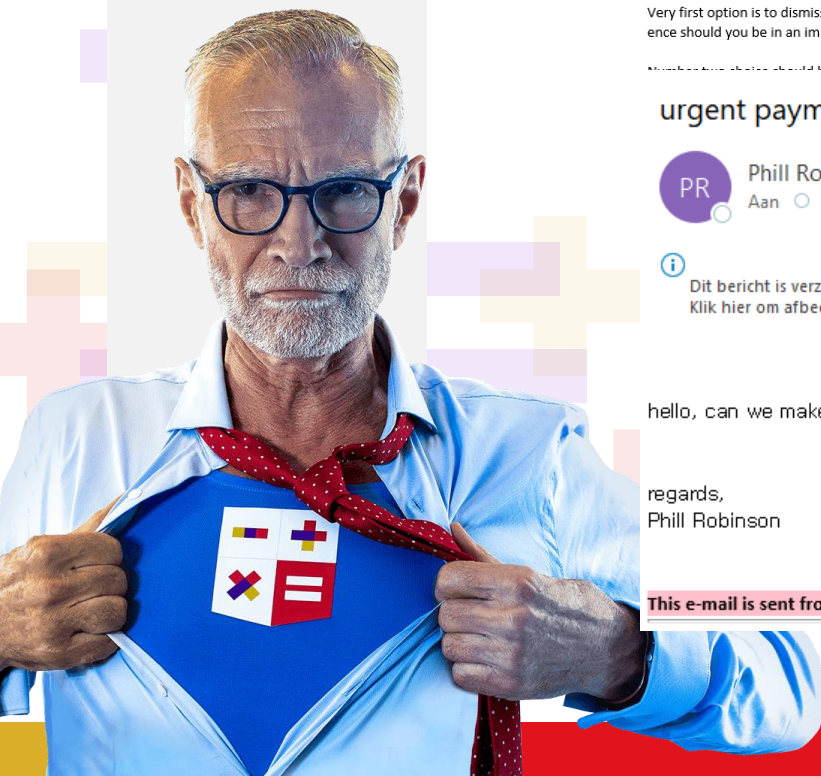
Dit bericht is verzonden met de prioriteit Hoog.

Klik hier om afbeeldingen te downloaden. Om uw privacy te beschermen, zijn enkele afbeeldingen in dit bericht niet automatisch gedownload.

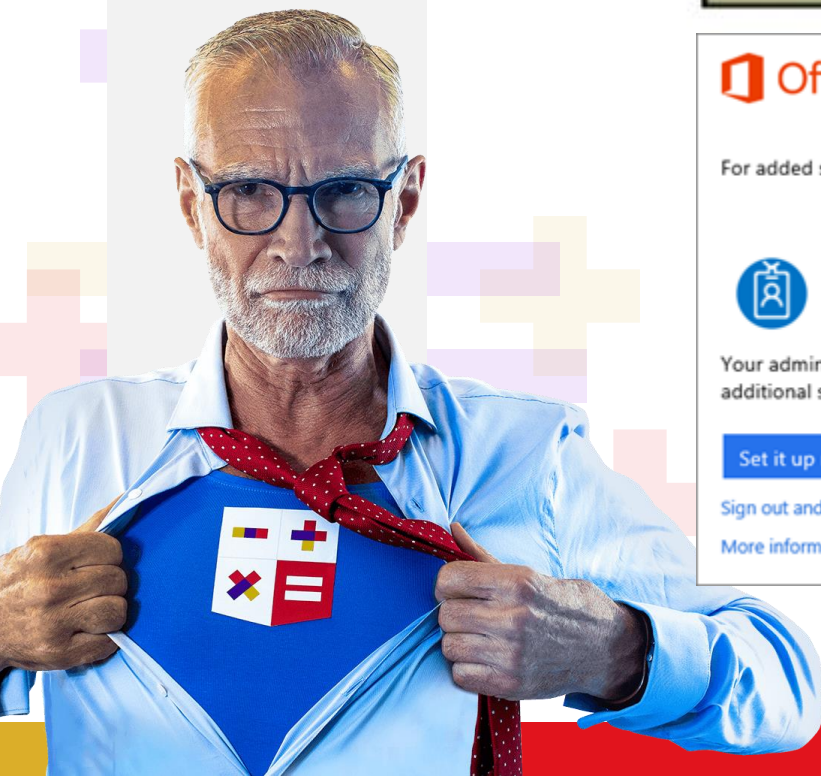
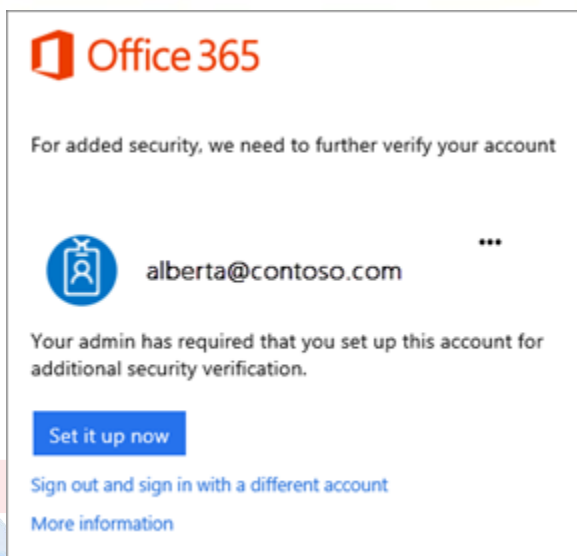
hello, can we make a SEPA payment of 10 500 euros today?

regards,
Phill Robinson

This e-mail is sent from an external email address. Please do not open attachments or click links from an unknown or suspicious origin. If you have any questions or concerns, please contact the IT Services team.



2. Phishing & wachtwoorden



exact
Live
2019

3. Malware / Ransomware



Vijf lessen

Zorg ervoor dat software-updates plaats vinden

- + Stel de updates niet uit
- + Indien automatisch updaten mogelijk is, maak hier gebruik van

Pas op voor verdachte e-mails en telefoontjes

- + Wees cynisch over links in e-mail / sms
- + Controleer elk verzoek om gevoelige informatie, ongeacht de bron

Pas goed wachtwoordmanagement toe

- + Wachtwoorden: Lang (of een zin), complex, niet herhaalbaar / herkenbaar
- + Vermijd persoonlijke referenties
- + Wachtwoord managers (Lastpass, Keypass) zijn aanbevolen. Deze zijn ook gratis te verkrijgen

Laat je eigendommen niet onbeheerd achter

- + Vergrendel altijd je apparaten, laptop (Windows-L), telefoon, etc.
- + In publieke ruimtes, laat ze niet onbeheerd achter

Bescherm gevoelige data

- + Overweeg altijd waar je je data op slaat. Niet elke tool, cloud is geschikt
- + Gebruik encryptie waar dat kan
- + Maak regelmatig backups



exact
Live
2019

Vragen?

