

# Security and the Internet: an ongoing struggle?



# SWITCH

Michael Hausding

[michael.Hausding@switch.ch](mailto:michael.Hausding@switch.ch)

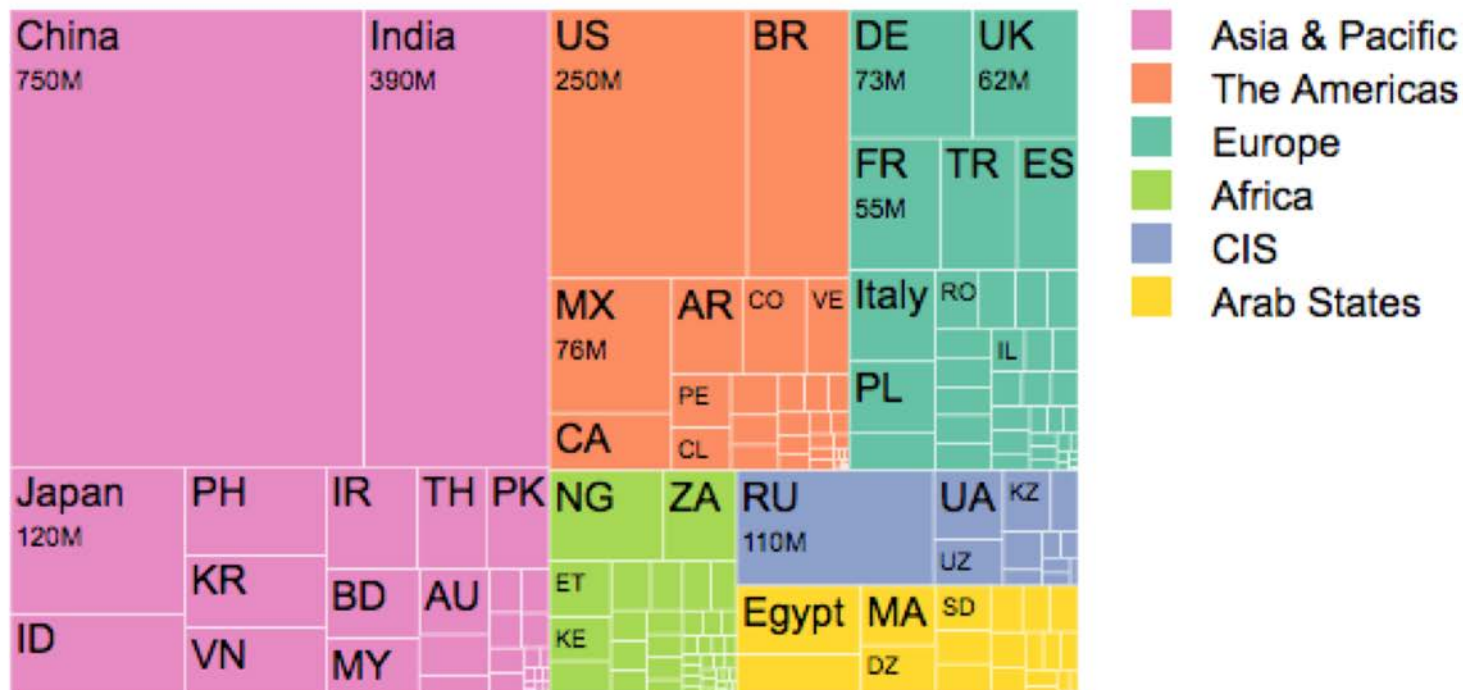
@mhausding

Eduhub Security Awareness Workshop  
Zürich, 15.8.2018

**Internet  
growth**



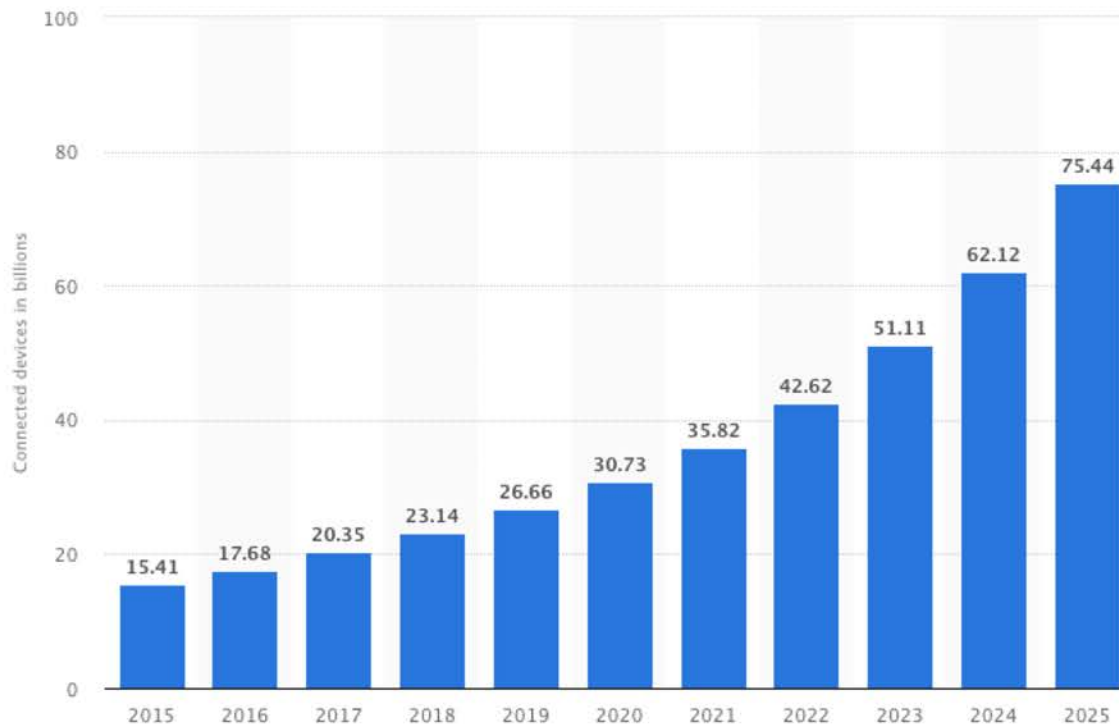
Total Internet users: 3,385 M



<https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx>

# Devices connected to the Internet

Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025 (in billions)



DOWNLOAD SETTINGS SHARE



DESCRIPTION SOURCE MORE INFORMATION

This statistic shows the number of connected devices (Internet of Things; IoT) worldwide from 2015 to 2025. For 2020, the installed base of Internet of Things devices is forecast to grow to almost 31 billion worldwide. The [overall Internet of Things market](#) is projected to be worth more than one billion U.S. dollars annually from 2017 onwards.



<https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/>

# Internet Crime

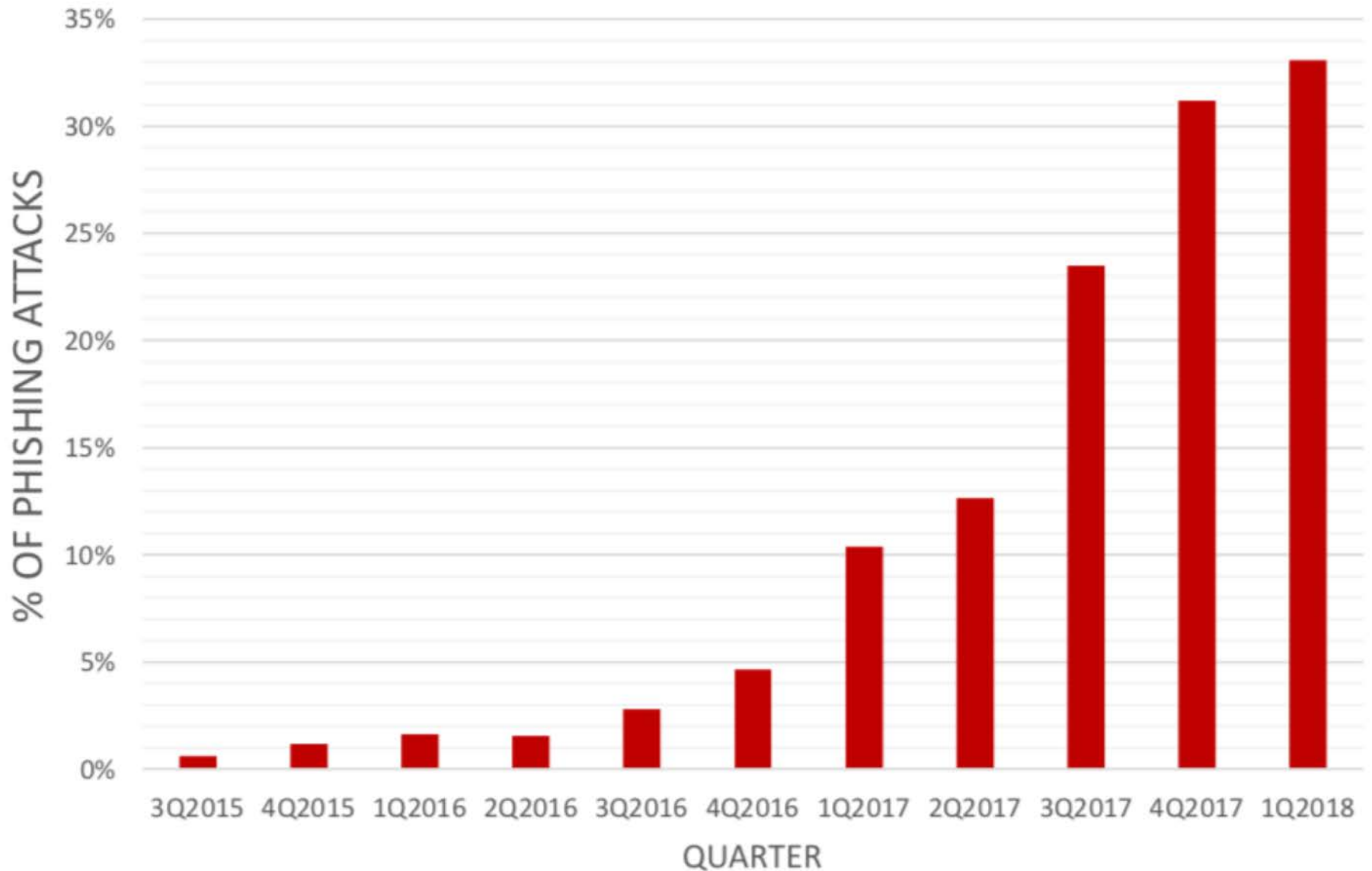
# Cybercrime daily (2016)

<b>Cybercrime</b>	<b>Estimated Daily Activity</b>
Malicious scans	80 billion
New malware	300,000
Phishing	33,000
Ransomware	4,000
Records lost to hacking	780,000

Table 1. Estimated daily cybercrime activity

<https://www.mcafee.com/enterprise/en-us/assets/reports/restricted/economic-impact-cybercrime.pdf>

# Phishing Sites Hosted on HTTPS





# Le Matin

## SPÉCIAL 42<sup>e</sup> PALÉO FESTIVAL NYON

RECHERCHE

E-PAPER



23°

SUISSE SPORTS FAITS DIVERS MONDE PEOPLE LOISIRS SOCIÉTÉ ÉCONOMIE HIGH-TECH AUTO SANTÉ PLUS

WEB HARD-/SOFTWARE JEUX IMAGES

**BREAKING SECURITY CONTROLS USING SUBDOMAIN HIJACKING**

### SONDAGE ETES-VOUS ACCRO À LA SÉRIE "GAME OF THRONES"?

- Oui, je dévore chaque épisode
- Non, je n'ai pas du tout accroché
- Euh... de quoi s'agit-il?

VOTER





# Actors



# Criminals



# Ransomware



Ooops, your files have been encrypted!

English

## What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

## Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled.

Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

## How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.

Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.

And send the correct amount to the address specified in this window.

After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

CMT from Mondays to Friday

Payment will be raised on

5/16/2017 00:47:55

Time Left

02:23:57:37

Your files will be lost on

5/20/2017 00:47:55

Time Left

06:23:57:37

[About bitcoin](#)

[How to buy bitcoins?](#)

[Contact Us](#)

Send \$300 worth of bitcoin to this address:



12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Copy

# Fake Webshop

**JUST DO IT.**

Währungen: Swiss Franc

Suchbegriff

STARTSEITE NIKE AIR FORCE 1 AIR JORDAN 5 IMPRESSUM & KONTAKT

THE ART OF ATTACK

nike online shop schweiz  
www.caution-de-loyer.ch

**Kategorien**

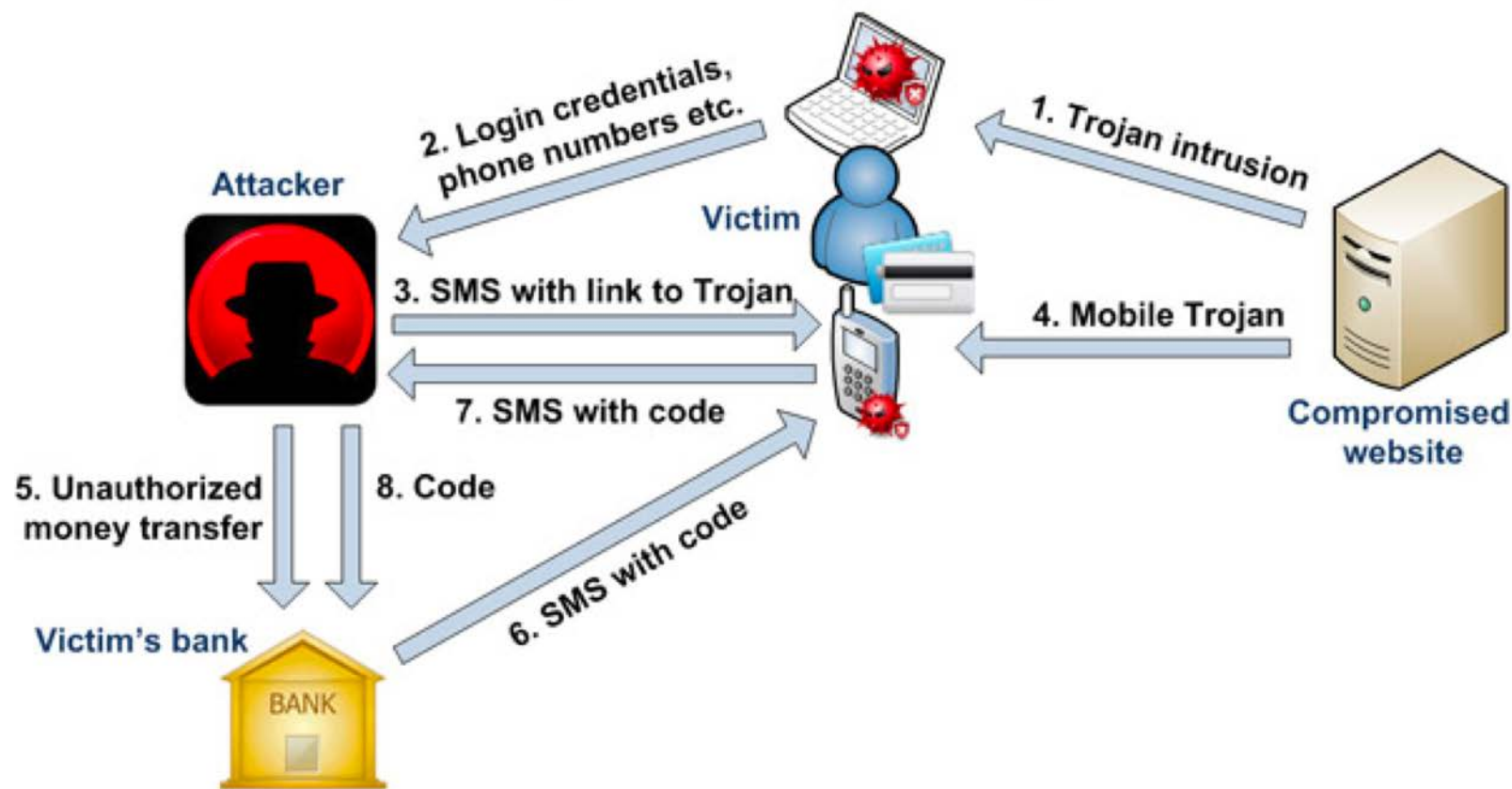
- 2016 Neue Artikel
- 2016 Nike Air Max
- New Jordans
- Nike Air Foamposite
- Nike Air Force 1
- Nike Air Huarache Damen
- Nike Air Huarache Herren
- Nike Air Jordan Damen
- Nike Air Jordan Herren

**NEUE ARTIKEL IM AUGUST**

2016 Nike Air Jordan 13 Retro Low "Qual 54" Sneakers Schwarz Khaki AJ Männer Schuhe	2016 Nike Air Jordan 13 Retro Low "Qual 54" Sneakers Weiss Universität Blau AJ Männer Schuhe	2016 Nike Air Jordan 30th XII 13 Retro "Hornissen" Low Frauen Schuhe Weiss Silber-Navy-Türkis 310810
CHF201.34 <b>CHF82.06</b>	CHF202.29 <b>CHF82.06</b>	CHF198.31 <b>CHF81.08</b>

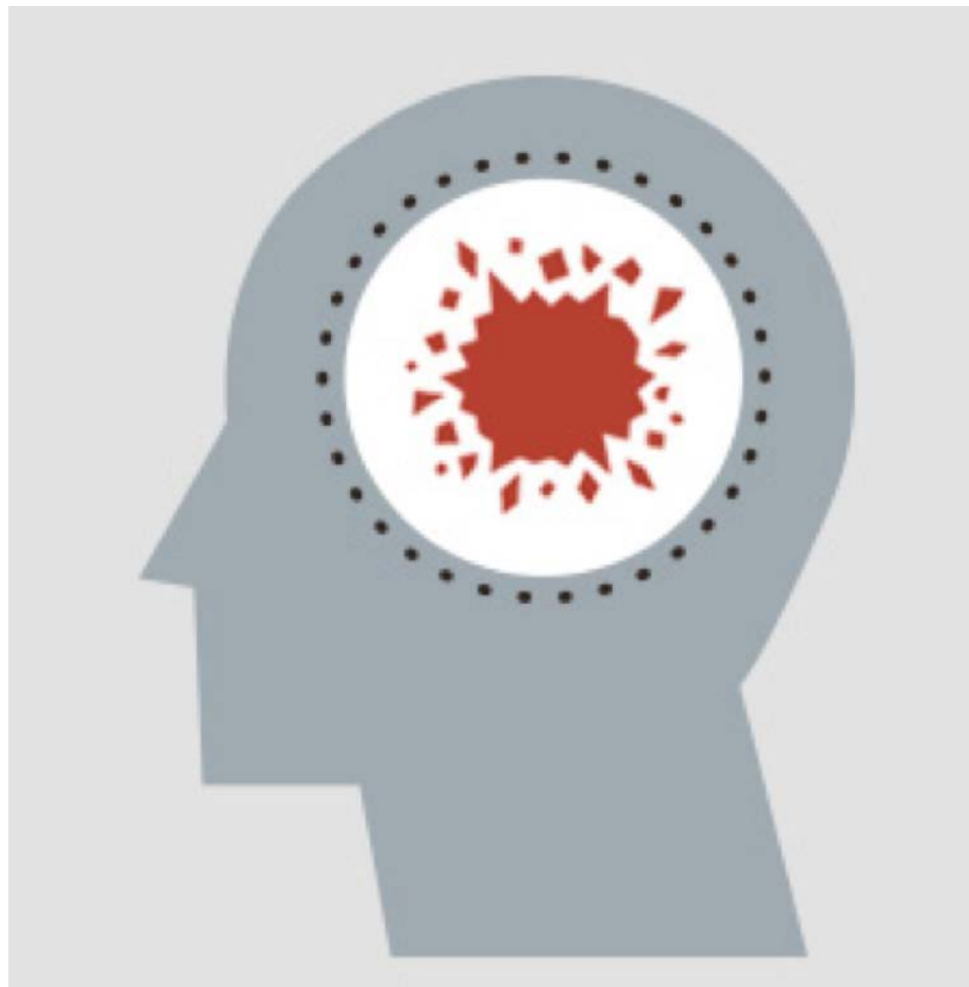
# Ebanking trojans

## Example of banking Trojan attack





# Hacktivists







«KEEP ON FIRING!»

SWITCH

# Postfinance schlägt zurück: Grössere Server gegen Wikileaks-Hacker

azNetz • Zuletzt aktualisiert am 7.12.2010 um 11:21 Uhr



## Operation: Payback



«Operation: Payback»

So nannten die Hacker ihren Vergeltungsschlag gegen Postfinance.

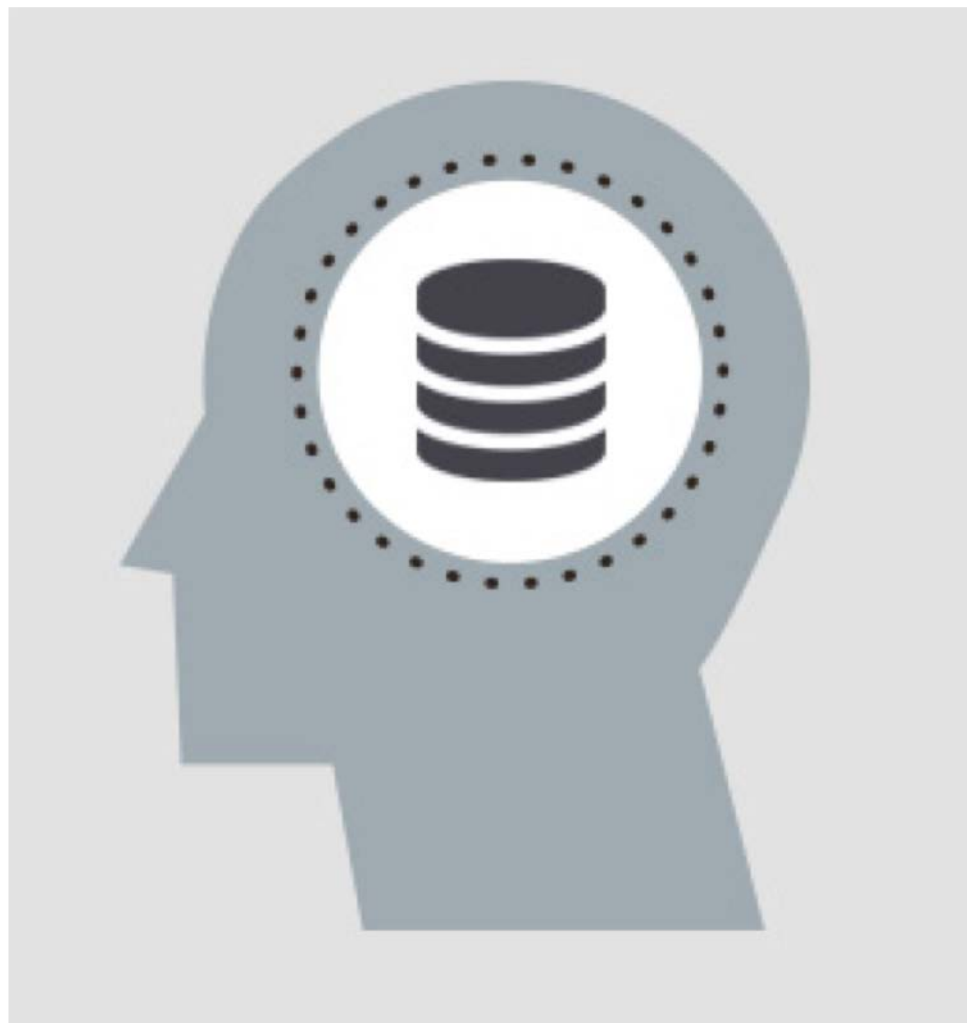
© Keystone

---

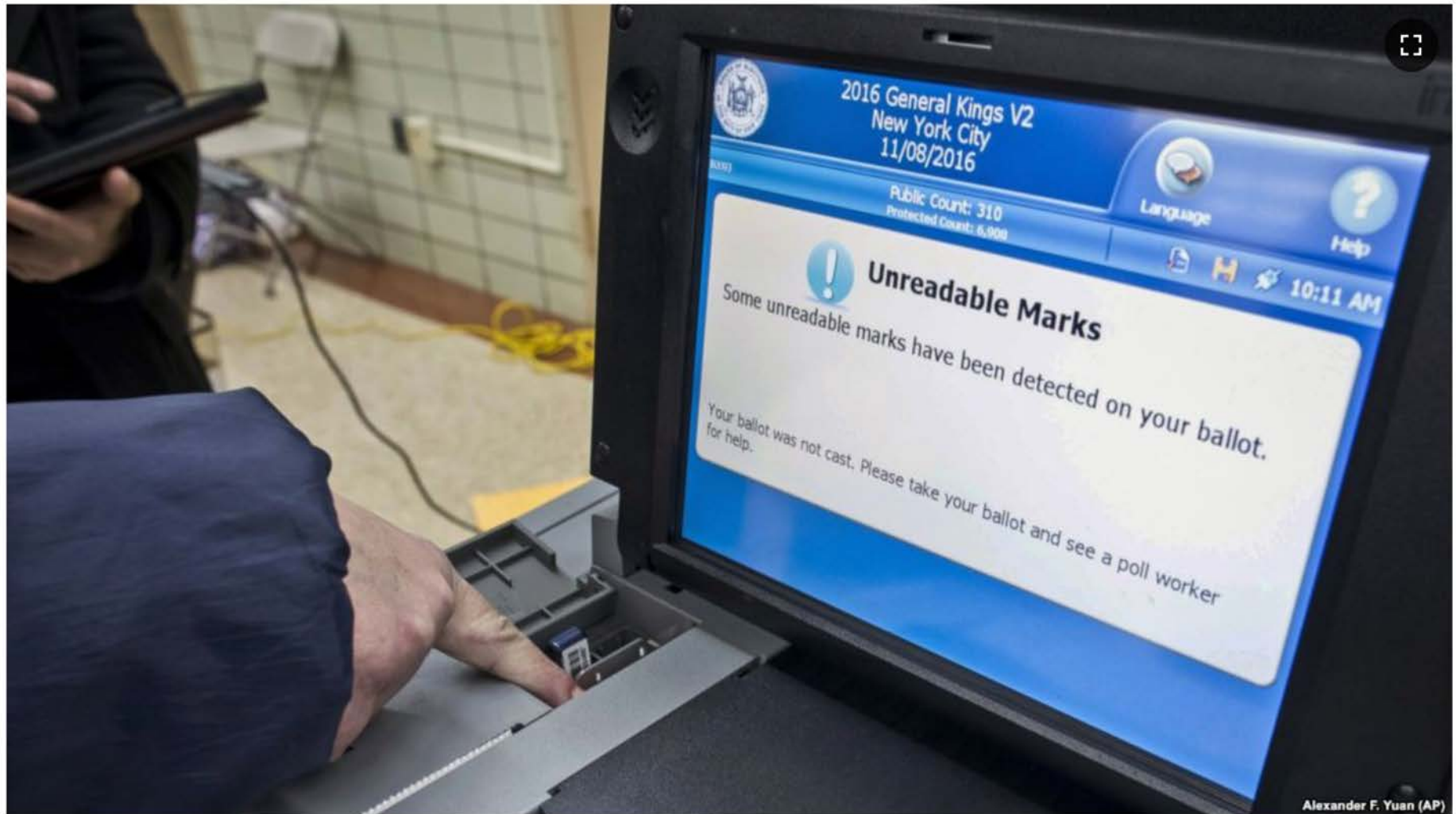
**Nachdem Postfinance das Konto von Julian Assange geschlossen hat, war die Webseite der Bank nun Ziel von Hackern. Seit über zehn Stunden geht fast nichts**



# State Sponsored Actors



# Russian Hackers Attacked U.S. Voting Systems in 2016, Senate Panel Says



A New York City Board of Elections ballot scanning machine is shown at a polling station in Brooklyn.

# Insiders





# Research: Half of Enterprises Suffered Insider Attacks in Last 12 Months

By: Chris Preimesberger | November 20, 2017

Survey is based on a comprehensive online survey of 472 cybersecurity professionals, which provides deep insight into current security trends.



People are often surprised to find out that most damaging security threats do not originate from malicious outsiders or malware but from trusted employees inside a company or value chain. Sometimes the person you think most trustworthy inside a company turns out to be the mole.

It's all about human nature. None of us can ever read people's minds and know the true and/or secret motivations that cause a trusted employee to go south. Not even the best security scheme can stop a malminded insider from doing damage.

[The 2018 Threat Report](#), released Nov. 20 and conducted by Crowd Research Partners, clearly indicates that the vast majority of companies and government agencies believe that

<http://www.eweek.com/security/research-half-of-enterprises-suffered-insider-attacks-in-last-12-months>




**Tactic  
Techniques  
Procedures  
(TTP)**

# Phishing

On 15.08.2018 11:25 the following URL was visited:  
<https://idp.epfl.ch.lli.nl/idp/profile/SAML2/POST/POST/SSO3jsessionid%3D5A169F8F2C4A062668F1C1A6009C6882.execution%3De1s1/>

SWITCHaai

 EPFL  
ÉCOLE POLYTECHNIQUE  
FÉDÉRALE DE LAUSANNE

**EPFL Shibboleth IdP**

In order to access the service **EZ-Proxy EPFL Bibliothèque**, you need to authenticate first.

Enter your username and password below, then click on the **Login** button to continue.

**Username:**

**Password:**

[▶ Options for personal data protection](#)

[> Forgot your Gaspar password? : call 1234 @ EPFL](#) [> Need Help?](#)

<https://www.switch.ch/de/phishing/report-phishing/>



# Malware

===**DHL EXPRESS**===

**ATTN:**

Dear Customer,

Your parcel has arrived at our office but there was some delays delivering to your address. Herein are your documents and copy of **DHL** receipt for your reference.

Please check the attached to confirm accordingly if your address is correct, before we submit to our outlet officer for dispatch to your destination.

**Class: Package Services**  
**Service(s): Delivery Confirmation**  
**Status: Notification sent**

**NOTE:** Please check the details carefully .  
Dispatch Department **DHL** Express.

===**DHL EXPRESS**===

**COURIER SERVICE** © 2017

[www.dhl.com](http://www.dhl.com)

Under no circumstances shall this information or the information contained in any e-mail constitute a binding agreement to carry or for provision of carriage services whether with the listed or alternative carriers or vessels. The carrier may, in its absolute discretion, at any time and without prior notice, change the arrangement listed or make alternate arrangement or decline a booking. We recommend you to check with the carrier for any changes. The actual provision of carriage services is subject to the final acceptance of the carrier and subject to the availability of the carrier's equipment and vessel and subject to the terms and conditions set out in the carrier's standard bill of lading.

**Defense**

# Information Security

- **Firewalls**
- **Access Control**
- **Network Security**
- **Encryption**
- **Intrusion Detection**
- **Incident Response**

*Cybersecurity  
is a shared  
responsibility*

Unknown

# User Awareness

- **Backup**
- **Updates**
- **Strong Passwords - 2FA**
- **Get Professional Support**
- **Stop.Think.Connect.**