SOCIAL ENGINEERING

SANITA MEIJERE

09.11.2022

MEETING A NEW INDIVIDUAL

FRAUDULENT ACTIVITIES

- Shopping - Facebook ads, fake stores and auctions
- Job offers
- Romance
- Old friends – call back
- Fake invoices – use defined payments
- Fake investment opportunities – consult experts, e.g. Supervisory bodies
- Physical security

HOW TO RECOGNIZE FRAUDSTER

- Fake ID, phone number, email, foreign language, grammar mistakes
- Preparation
- Unsuitable time for call
- Manipulating (sad event, loss of money, problems with family members)
- Demanding
- Goal oriented

PASSWORD I

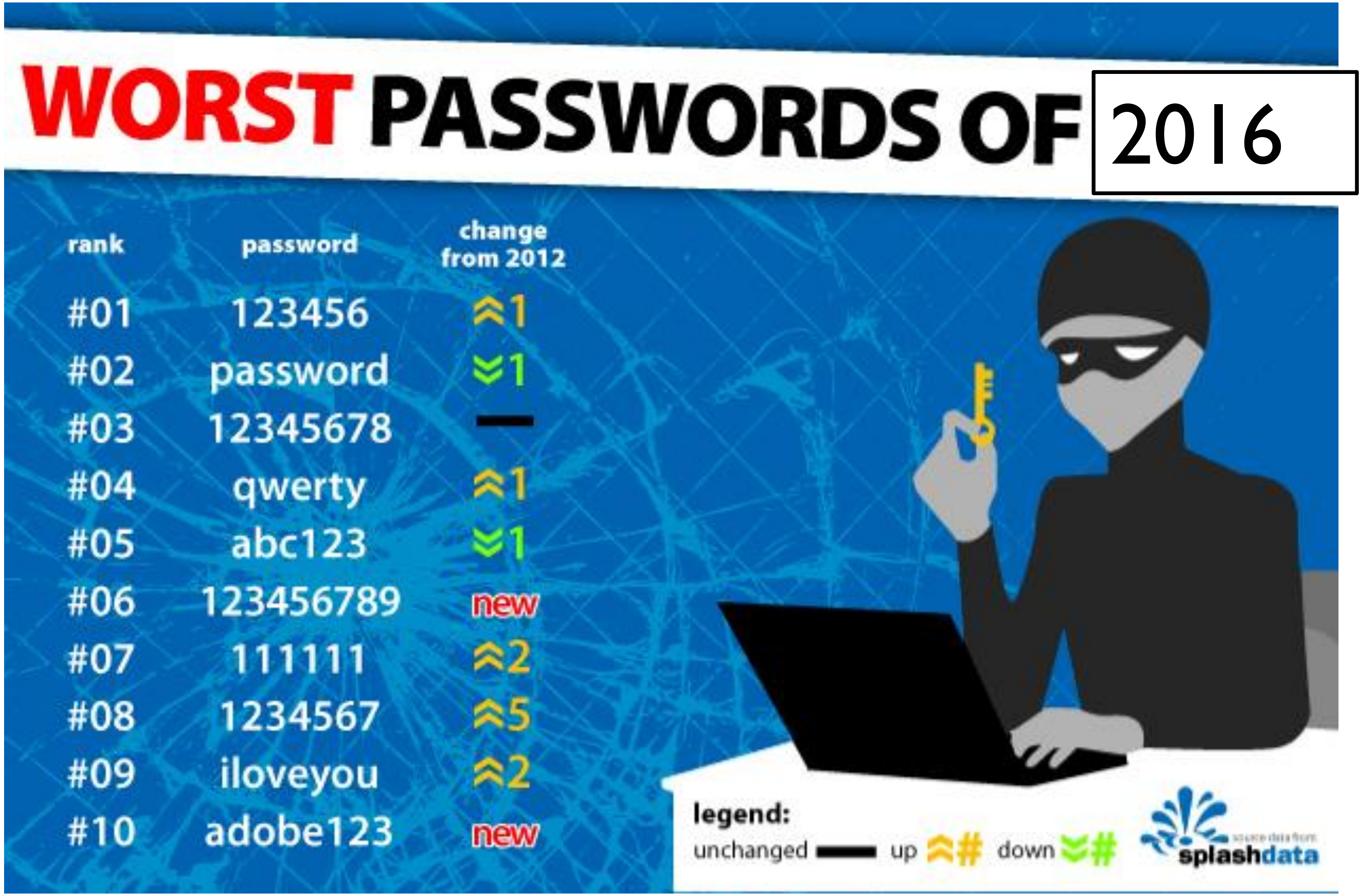
- Don't share your password!
- Avoid predictable passwords!
- Don't let your Web browser remember your passwords!
- Change passwords periodically!

30 - 90

PASSWORD II SECURE PASSWORDS

- Use **8 / 12** / **15** characters **minimum**
- **Uppercase** & **Lowercase** letters
- **Numbers**
- Special **symbols**

Symbol	**6 character password**	**7 character password**
#	9.7 sec	97 sec
Lower case letters	50 min	22 h
Lower & upper case letters	53 h	116 days
All 95 symbols	2 years	252 years



WORST PASSWORDS OF 2016

rank	password	change from 2012
#01	123456	↑1
#02	password	↓1
#03	12345678	—
#04	qwerty	↑1
#05	abc123	↓1
#06	123456789	new
#07	111111	↑2
#08	1234567	↑5
#09	iloveyou	↑2
#10	adobe123	new

legend:
unchanged — up ↑# down ↓#

source data from
splashdata

EMAILS

EMAIL SECURITY I SPAM

- Do not reply to SPAM!
- Do not spread SPAM!
- Do not forward chain letters!
- Never try to unsubscribe from SPAM!

EMAIL SECURITY II Junk

Check for valid e-mails accidently filtered to the Junk!

EMAIL SECURITY III SPYWARE

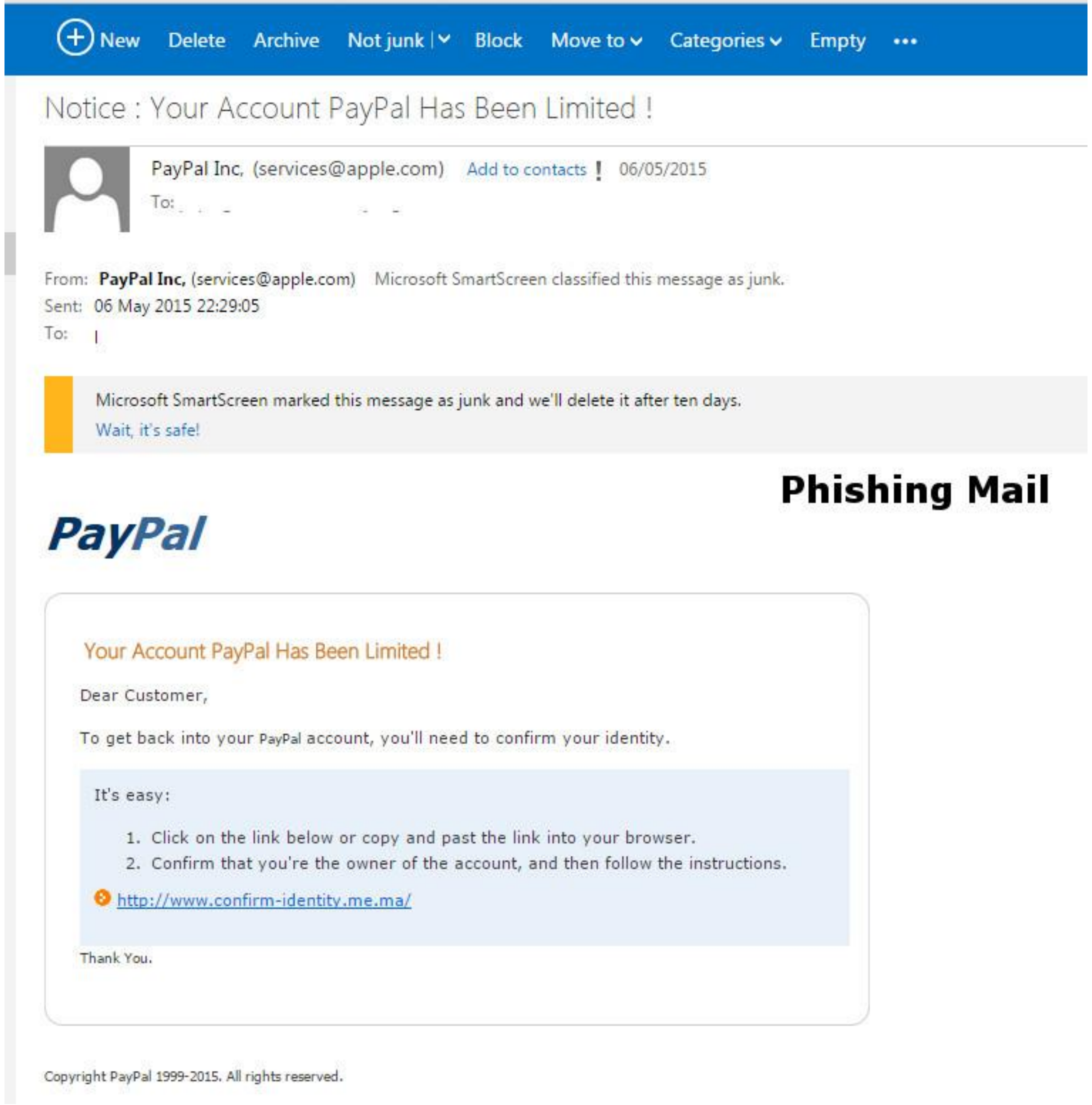
- Never click on a link/picture that is in SPAM!
- Never open an attachment in SPAM!

If it's suspicious, don't open!

- Attachments with a suspicious file extension (*.exe, *.vbs, *.bin, *.com, or *.pif)
- Unusual topic lines; "Your car?"; “You may have already won!"; “IMPORTANT"; "Oh!"; "Nice Pic!"; "Very Funny!", etc.

E-MAIL SECURITY IV PHISHING SCAMS

E-Mail pretending to
be from trusted names
requesting your login INFO etc.



Notice : Your Account PayPal Has Been Limited !

PayPal Inc, (services@apple.com) Add to contacts 06/05/2015

To:

From: **PayPal Inc,** (services@apple.com) Microsoft SmartScreen classified this message as junk.

Sent: 06 May 2015 22:29:05

To:

Microsoft SmartScreen marked this message as junk and we'll delete it after ten days.

Wait, it's safe!

Phishing Mail

PayPal

Your Account PayPal Has Been Limited !

Dear Customer,

To get back into your PayPal account, you'll need to confirm your identity.

It's easy:

1. Click on the link below or copy and past the link into your browser.
2. Confirm that you're the owner of the account, and then follow the instructions.

http://www.confirm-identity.me.ma/

Thank You.

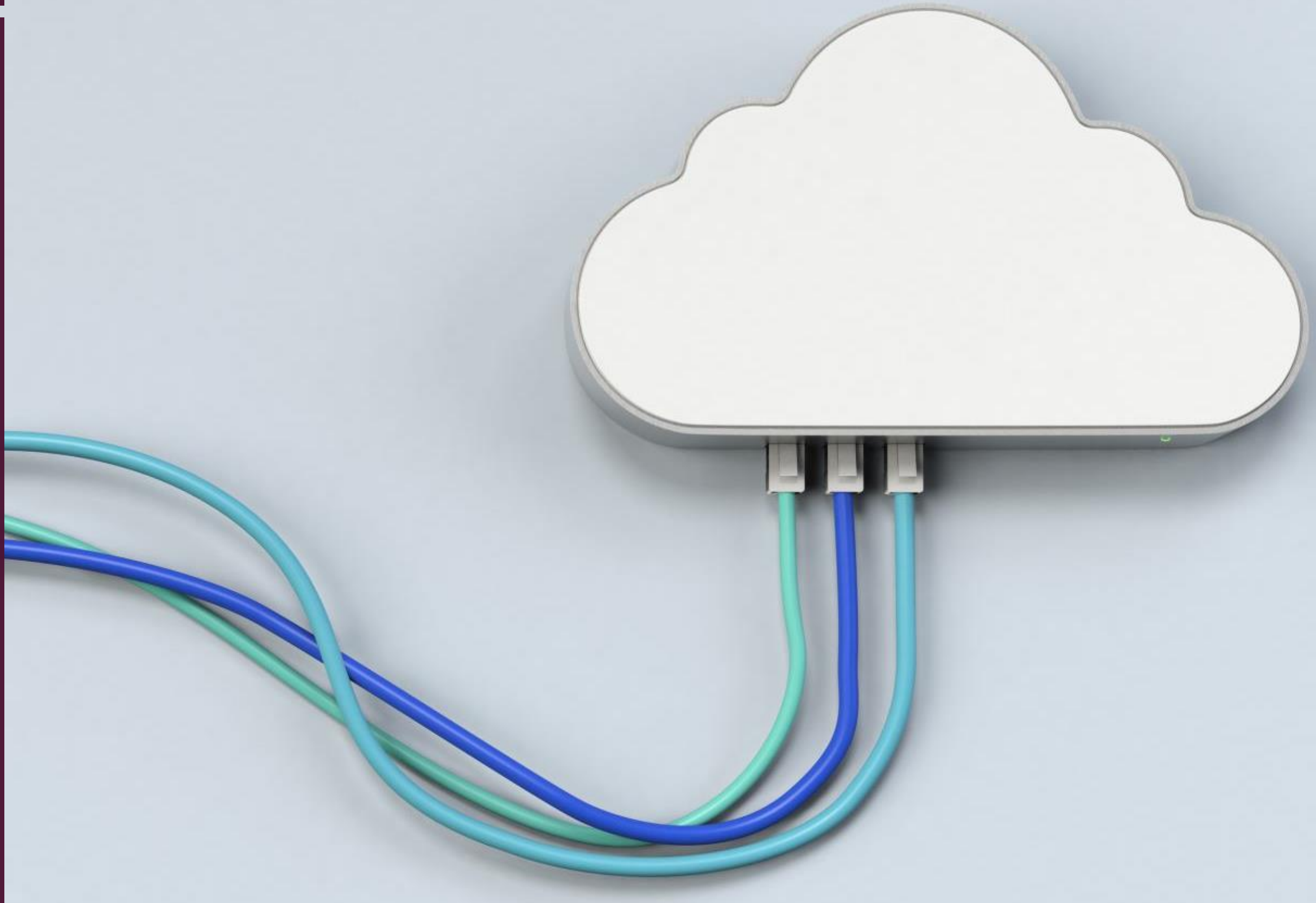
Copyright PayPal 1999-2015. All rights reserved.

DEVICES

SECURITY FOR WIRELESS DEVICES

Disable Wi-Fi module of Your portable devices while Wi-Fi is not in use in order to minimize risks of connecting to malicious hotspots

(& save battery life)

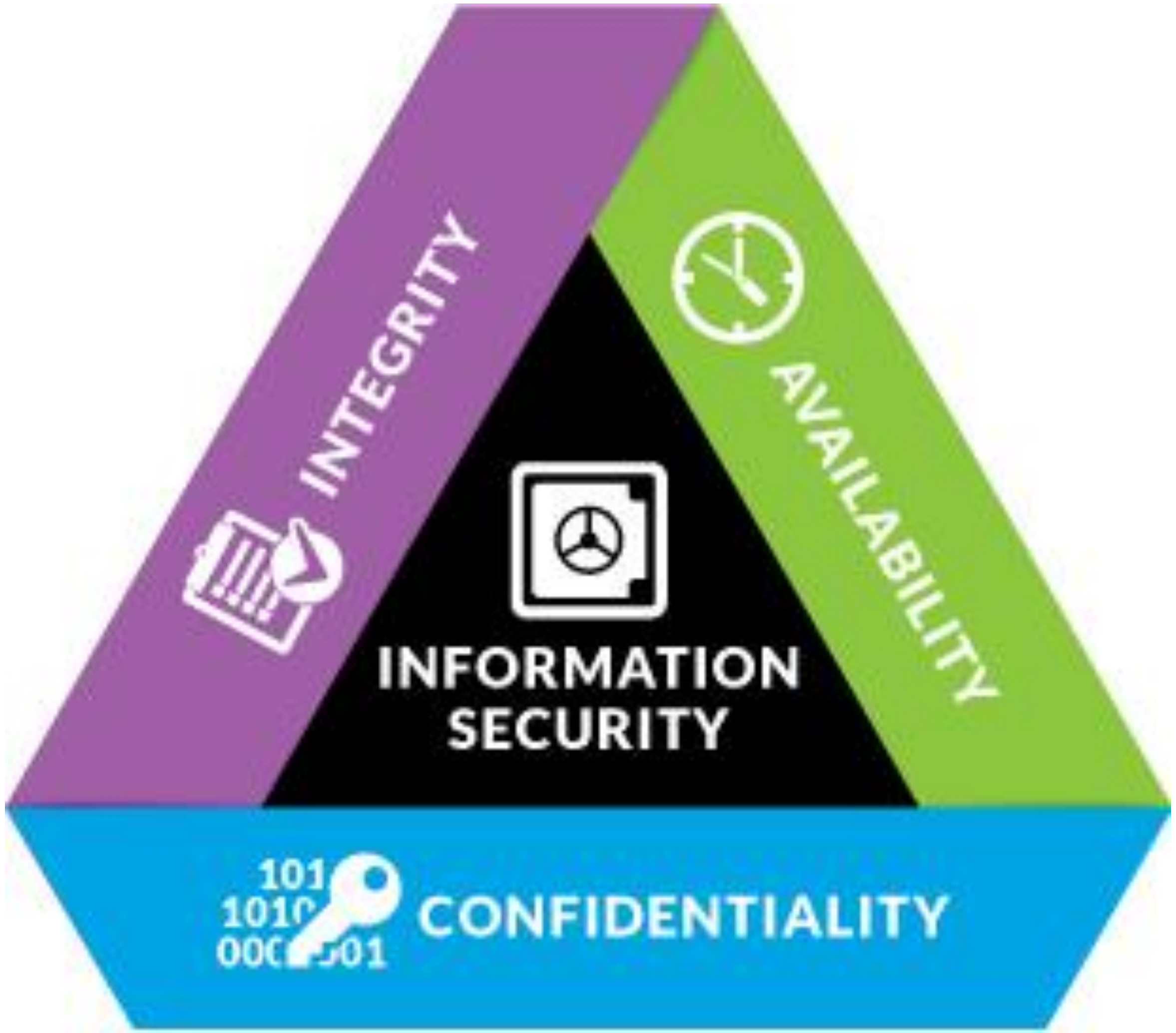


GENERAL

- **Log off** workstations before leaving at the end of your working hours
- **Lock** computer screen while walking away even for 5 minutes
- Data **back – up**
- Use only **Genuine** software

COMPANY NETWORK AND INTERNET USE. AVOID:

- Adult sites
- Gambling sites
- Gaming sites
- Chat rooms


INTEGRITY
AVAILABILITY
INFORMATION SECURITY
101
1010
000 01
CONFIDENTIALITY

INFORMATION CLASSIFICATION

Public / not labeled

Company Confidential

Restricted

RESOURCES

- http://www.cert.org/

Thank you!

Q & A