levi nine
Technology Services

Information Security & GDPR

March 2019, Iasi

Alexandru Vornicu – Information Security Officer
Ionut Stanescu – Software Architect

AGENDA

01 Information Security

02 GDPR Overview

03 Architecture of Privacy

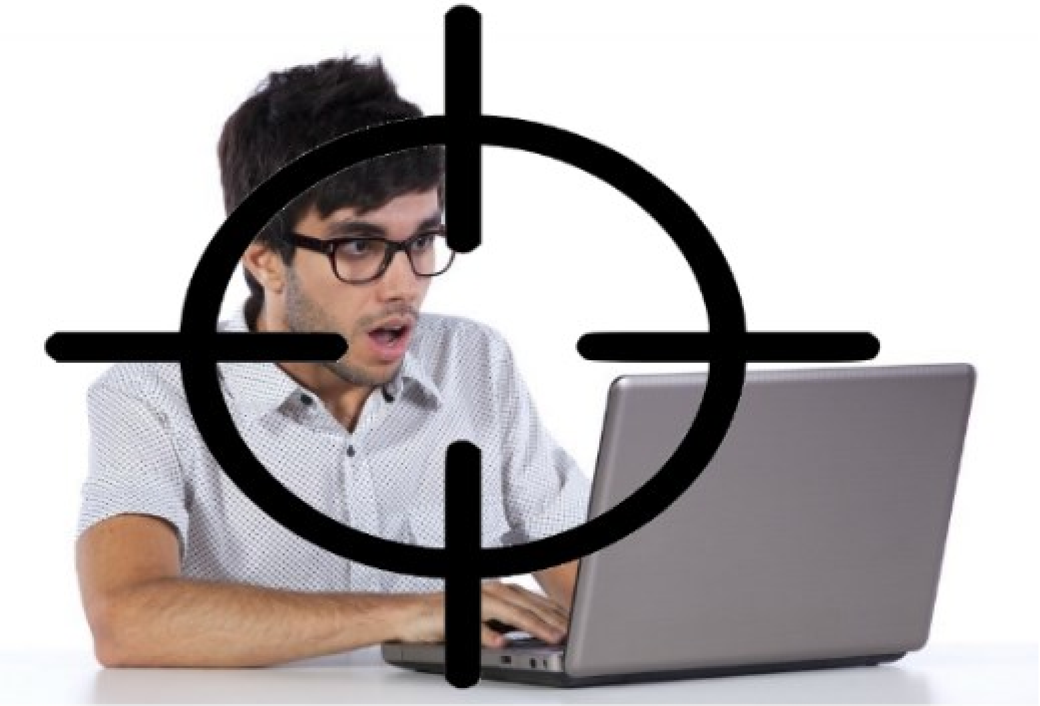
GO TO [HTTPS://KAHOOT.IT](https://kahoot.it) AND ENTER PIN

PART 1. INFORMATION SECURITY

IS INFORMATION SECURITY IMPORTANT?

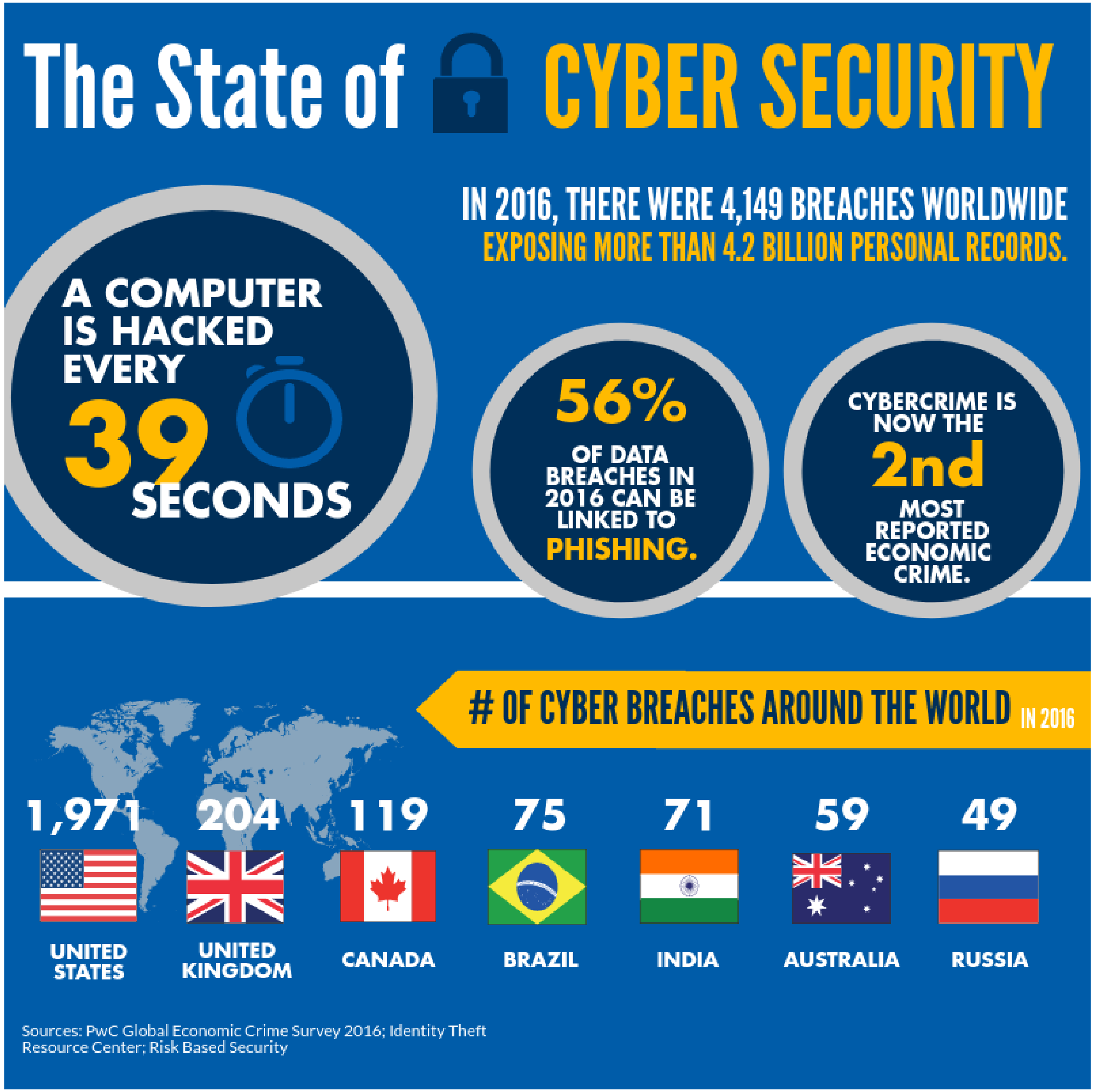
WHAT IS THE DANGER?

- Hackers do not hack systems any more…
- …they hack people!



CYBER SECURITY STATISTICS

- Never think it will never happen to me!



The State of CYBER SECURITY

IN 2016, THERE WERE 4,149 BREACHES WORLDWIDE EXPOSING MORE THAN 4.2 BILLION PERSONAL RECORDS.

A COMPUTER IS HACKED EVERY 39 SECONDS

56% OF DATA BREACHES IN 2016 CAN BE LINKED TO PHISHING.

CYBERCRIME IS NOW THE 2nd MOST REPORTED ECONOMIC CRIME.

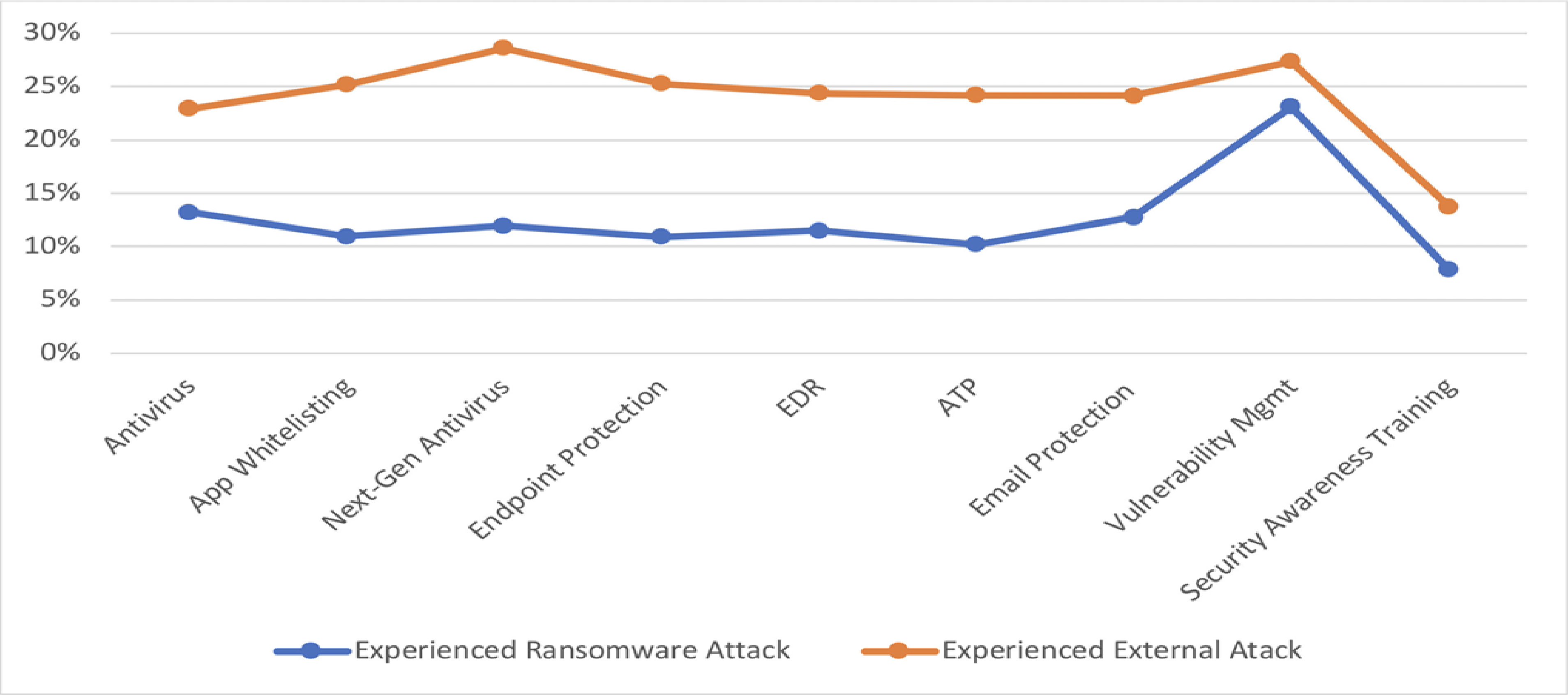
OF CYBER BREACHES AROUND THE WORLD IN 2016

UNITED STATES	UNITED KINGDOM	CANADA	BRAZIL	INDIA	AUSTRALIA	RUSSIA
1,971	204	119	75	71	59	49

Sources: PwC Global Economic Crime Survey 2016; Identity Theft Resource Center; Risk Based Security

HOW CAN WE BE SAFE?

- The best protection is awareness!
- Develop positive Security Habits
- Know vulnerabilities you are exposed to



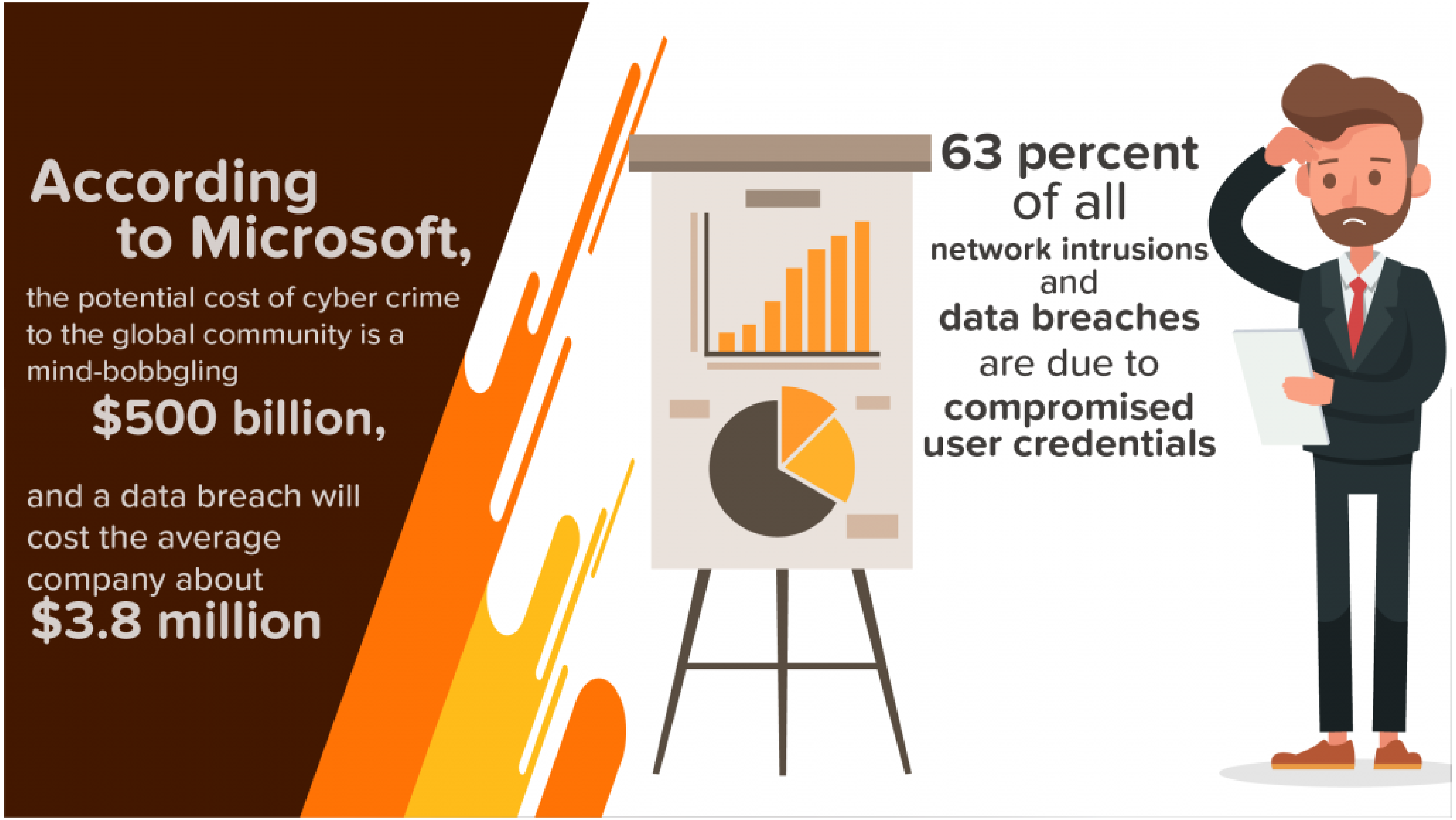
% of organizations experiencing attacks (by solution implemented)

ARE PASSWORDS IMPORTANT?

- What makes a password strong and secure?

I will not use the same password for everything
I will not use the same password for everything
I will not use the same password for everything
I will not use the same password for everything
I will not use the same password for everything
I will not use the same password for everything
I will not use the same password for everything
I will not use the same password for everything
I will not use the same password for everything
I will not use the same password for everything
I will not use the same password for everything

PASSWORD MANAGEMENT BEST PRACTICES



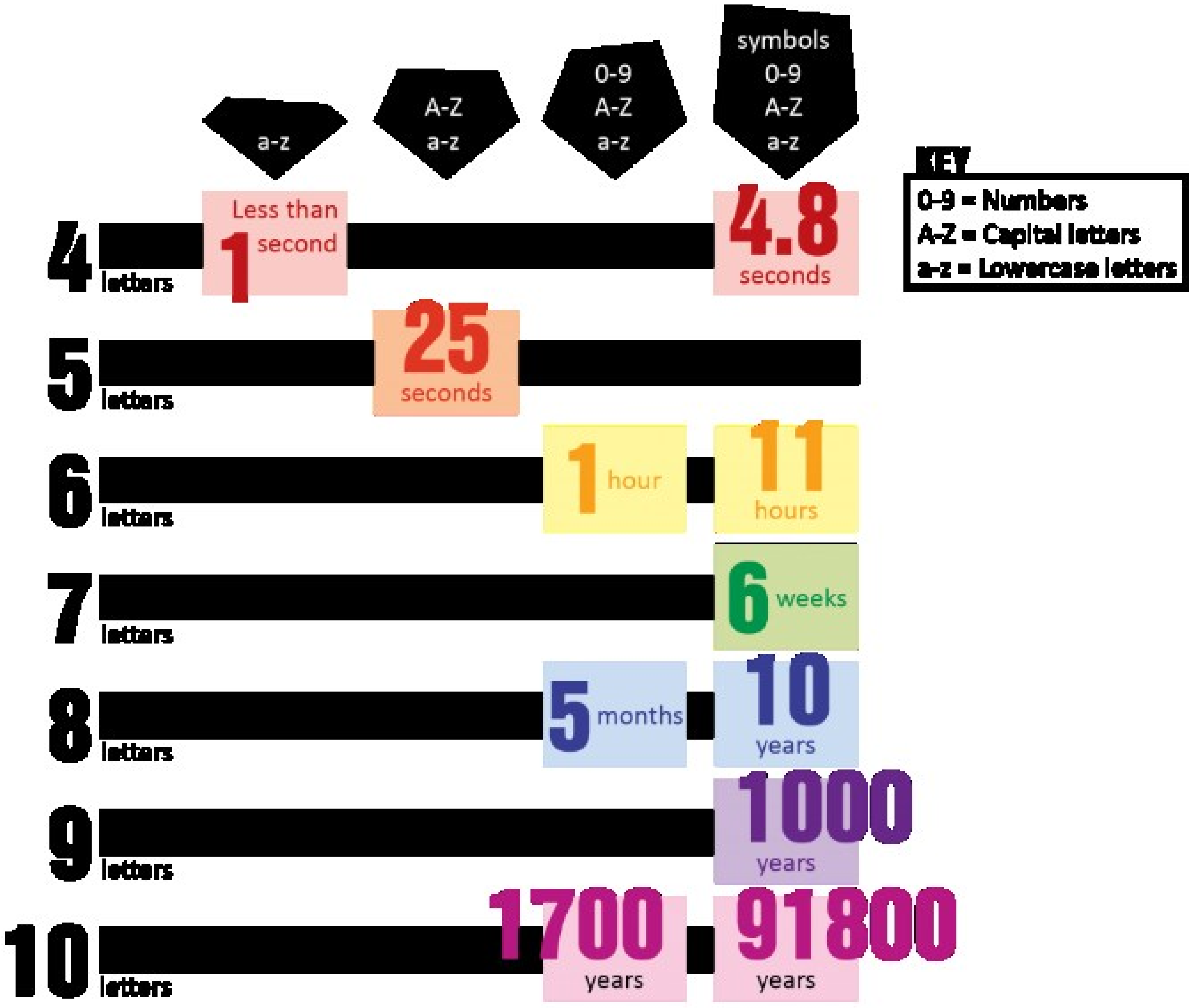
According to Microsoft, the potential cost of cyber crime to the global community is a mind-bobbgling **$500 billion,**

and a data breach will cost the average company about **$3.8 million**

63 percent of all **network intrusions** and **data breaches** are due to **compromised user credentials**

WHAT MAKES A PASSPHRASE STRONG?

- It's long
- It is a series of words that create a phrase
- Does not contain:
  - common phrases found in literature or music
  - words found in the dictionary
  - our user name, real name or company name
- It is significantly different from previous passwords or passphrases



	a-z	A-Z a-z	0-9 A-Z a-z	symbols 0-9 A-Z a-z
4 letters	Less than 1 second			4.8 seconds
5 letters		25 seconds		
6 letters			1 hour	11 hours
7 letters				6 weeks
8 letters			5 months	10 years
9 letters				1000 years
10 letters			1700 years	91800 years

KEY
0-9 = Numbers
A-Z = Capital letters
a-z = Lowercase letters

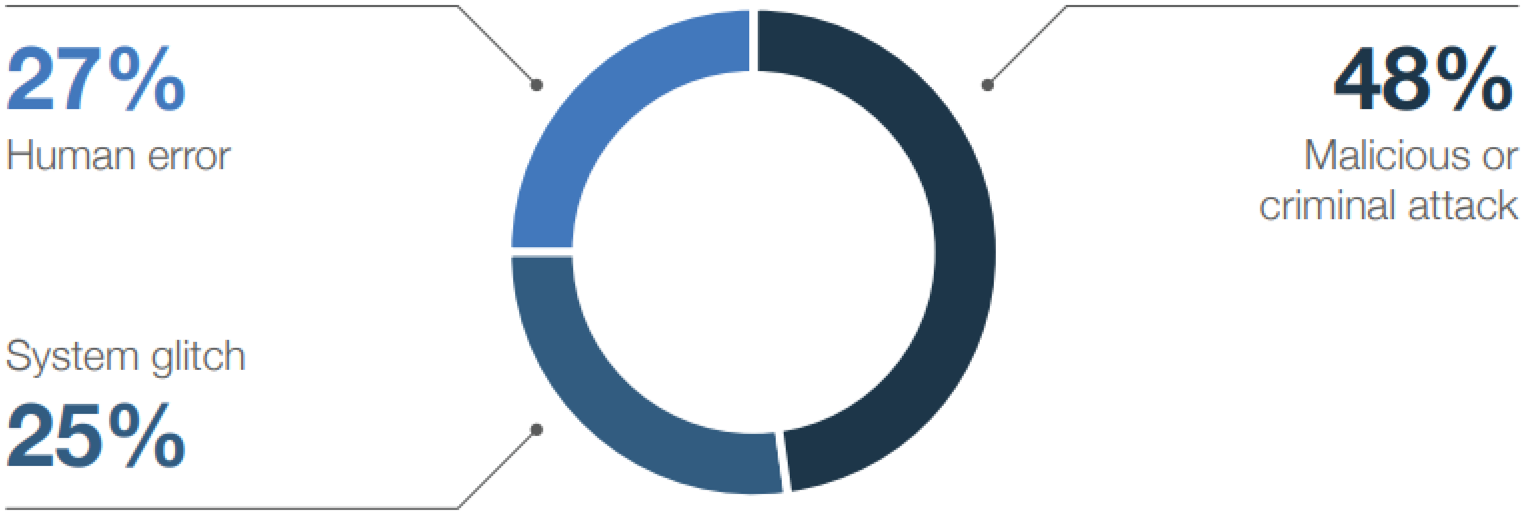
THREATS OVERVIEW

Malware

Phishing

Social Engineering

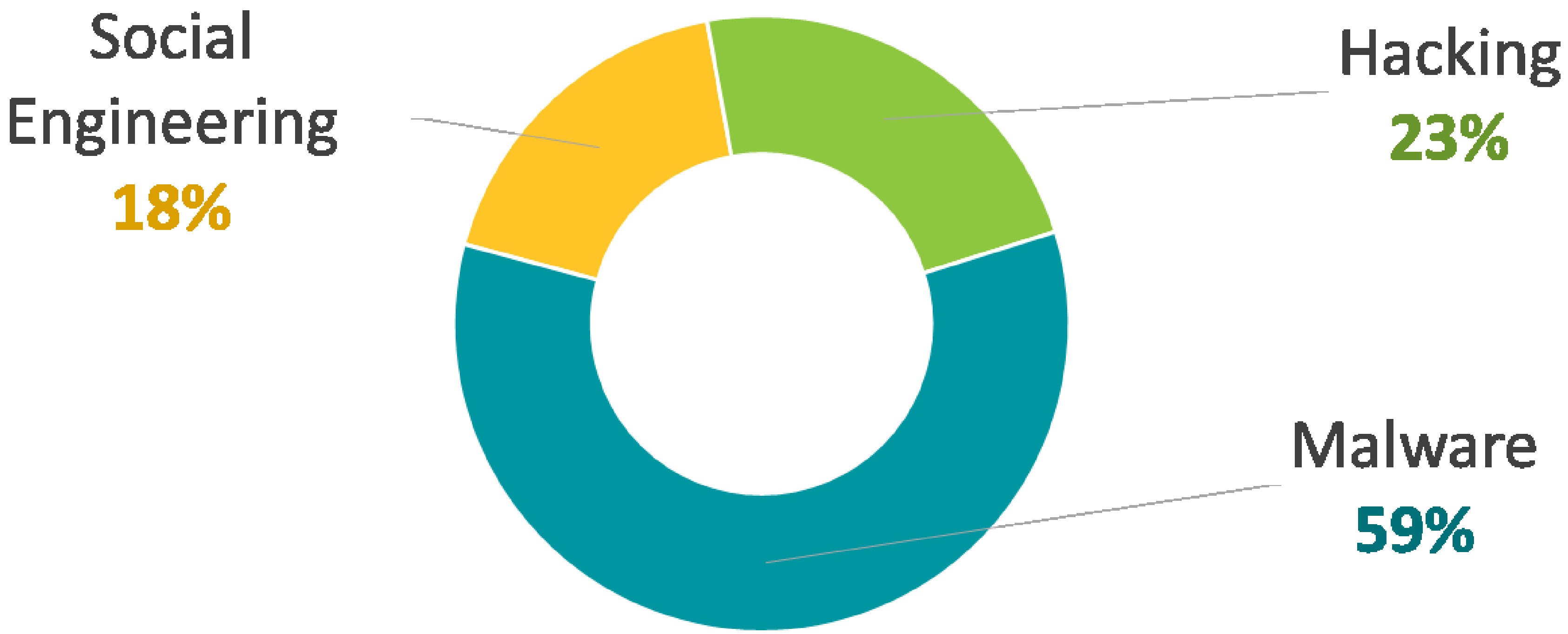
ROOT CAUSES OF DATA BREACHES



Ponemon Institute 2018 Cost of Data Breach Study: Global Analysis

Data Breach Breakdown

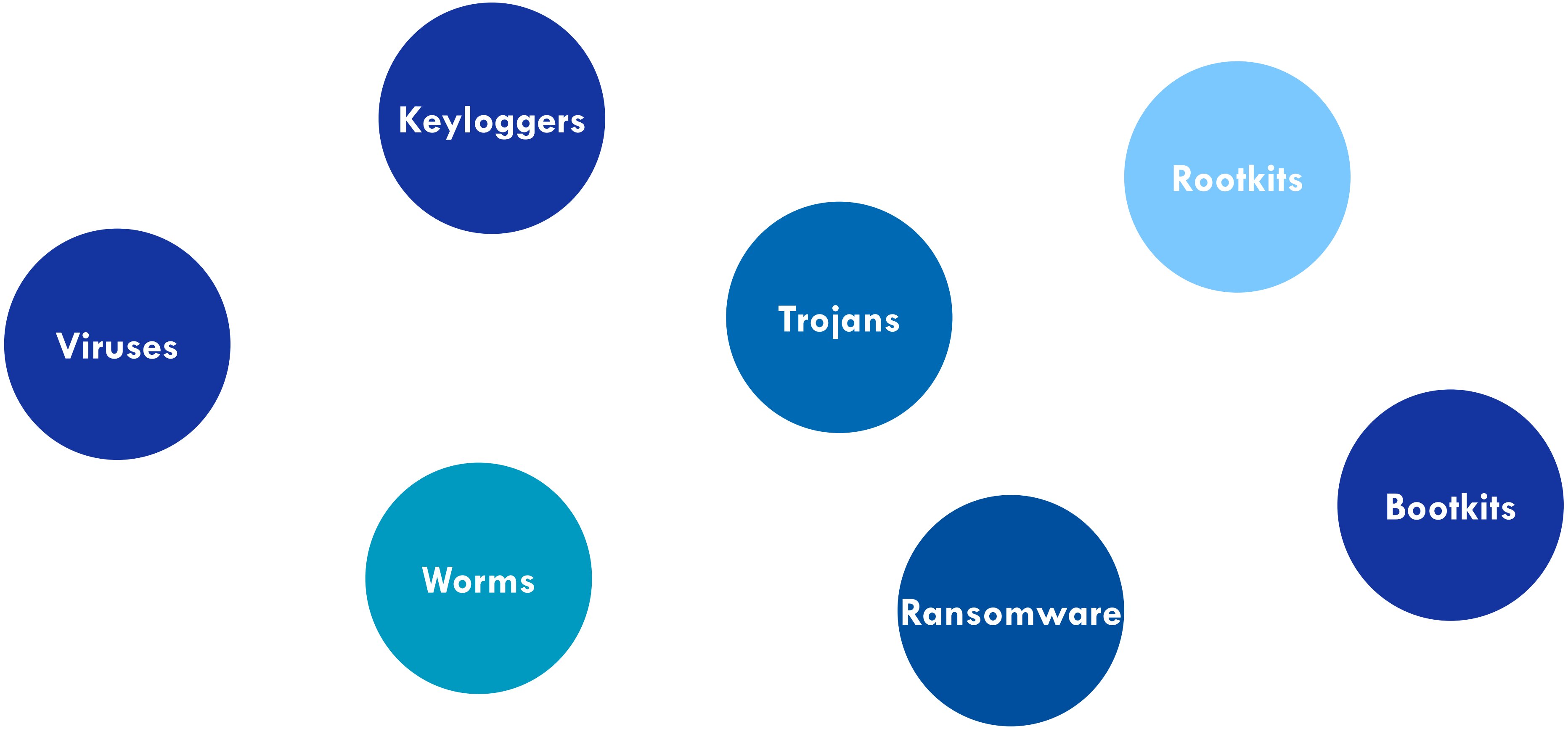
MALICIOUS BREACHES OVERVIEW



THREATS OVERVIEW

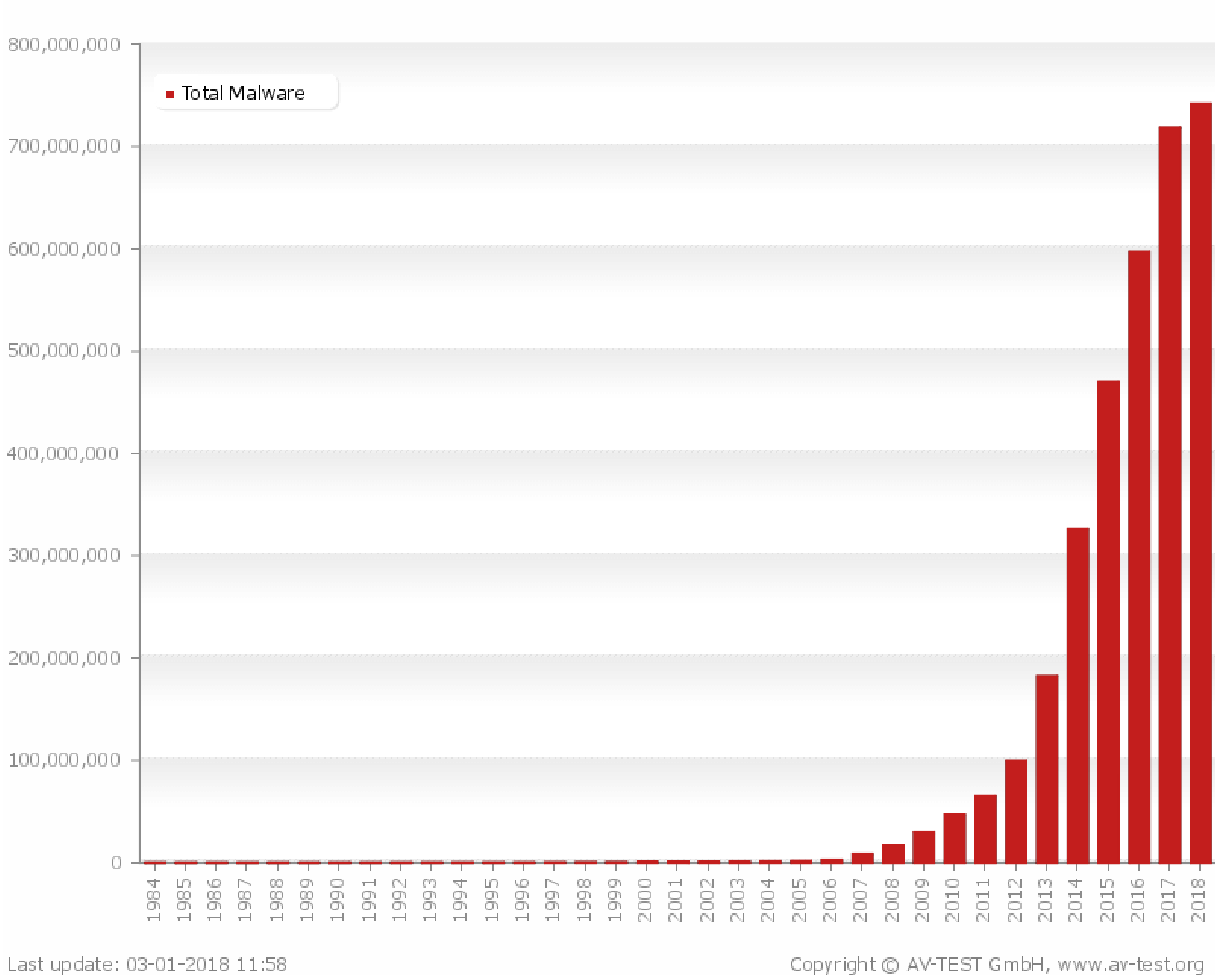
Malware

Malware includes numerous threat families, all with different names.



- Keyloggers
- Rootkits
- Viruses
- Trojans
- Bootkits
- Worms
- Ransomware

GROWTH OF MALWARE



MALWARE

- On average, 390,000 unique threats per day.
- Unique threats ≠ extremely dissimilar.
- Malicious threats are changed in the smallest amount possible to evade detection.
- Malicious threats are targeted in order to have the highest penetration (success) rate.

MALWARE

- Is malware on Windows only?
- Is malware on mobile phones?
- How does my system gets infected?
  - Clicking malicious links in email
  - Plugging in an unknown flash drive
  - Downloading malware masquerading as other software
  - Installing 3rd party apps directly from the internet instead of via official stores such as Google Play or Apple's App Store.

TOP TIPS TO AVOID MALWARE

1. Install (and keep updated) Antimalware software all devices.
2. Be careful what you plug in.
3. Be careful what you click.
4. Get awareness trainings.

THREATS OVERVIEW

Phishing

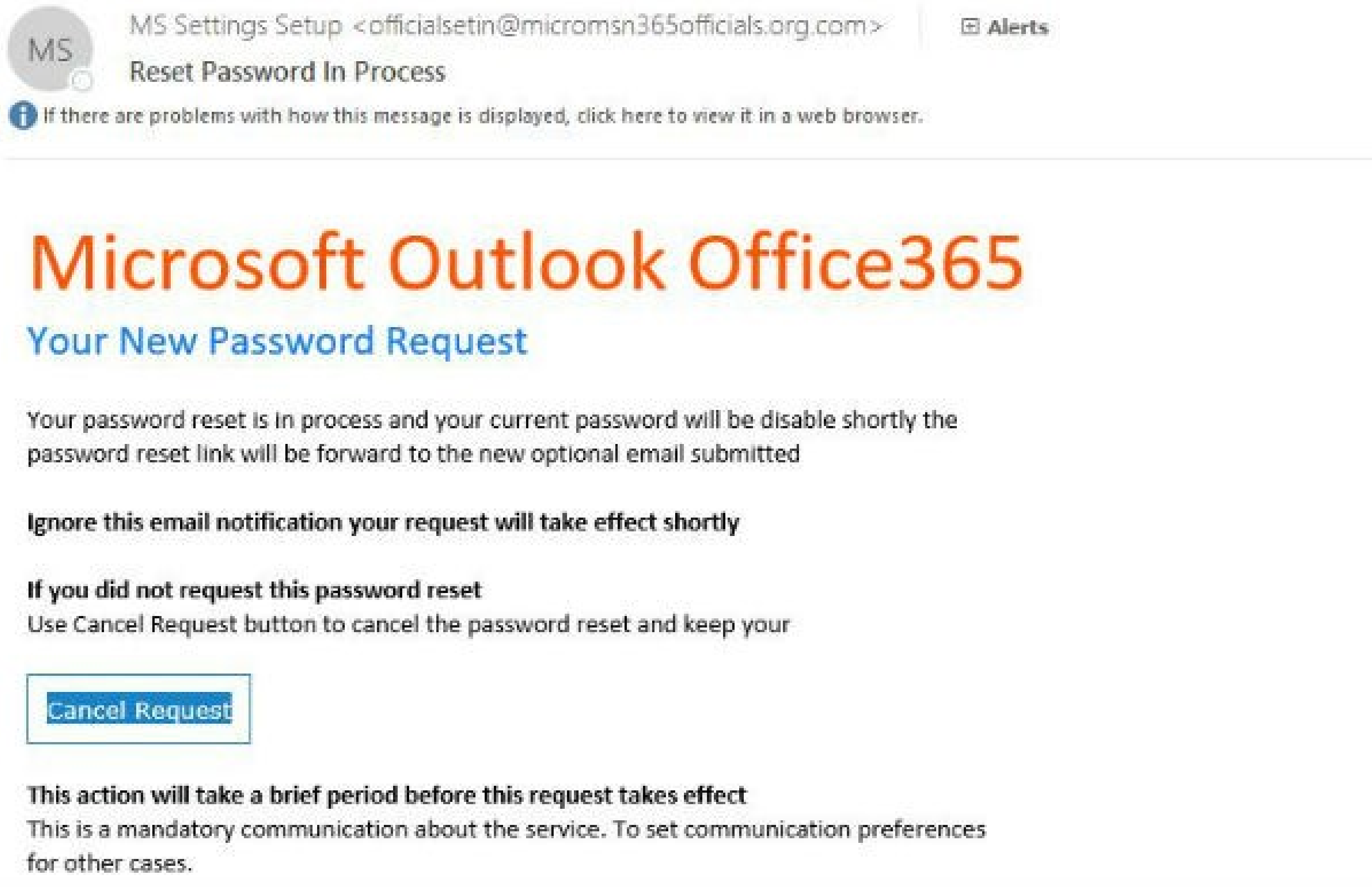
PHISHING? OR FISHING?

- Is the act of setting the bait (trap)…
- Casting it out into a wide ocean…
- Hoping that something bites that you can then hook.

PHISHING

- Intentionally deceiving someone by posing as a legitimate company.
- Typically, utilizes email by pretending to be a company or service requesting you to do something.
- Hoping that you click the link and fill out the requested info.

PHISHING EMAIL OR NOT?



MS Settings Setup <officialsetin@micromsn365officials.org.com>

Reset Password In Process

If there are problems with how this message is displayed, click here to view it in a web browser.

Microsoft Outlook Office365

Your New Password Request

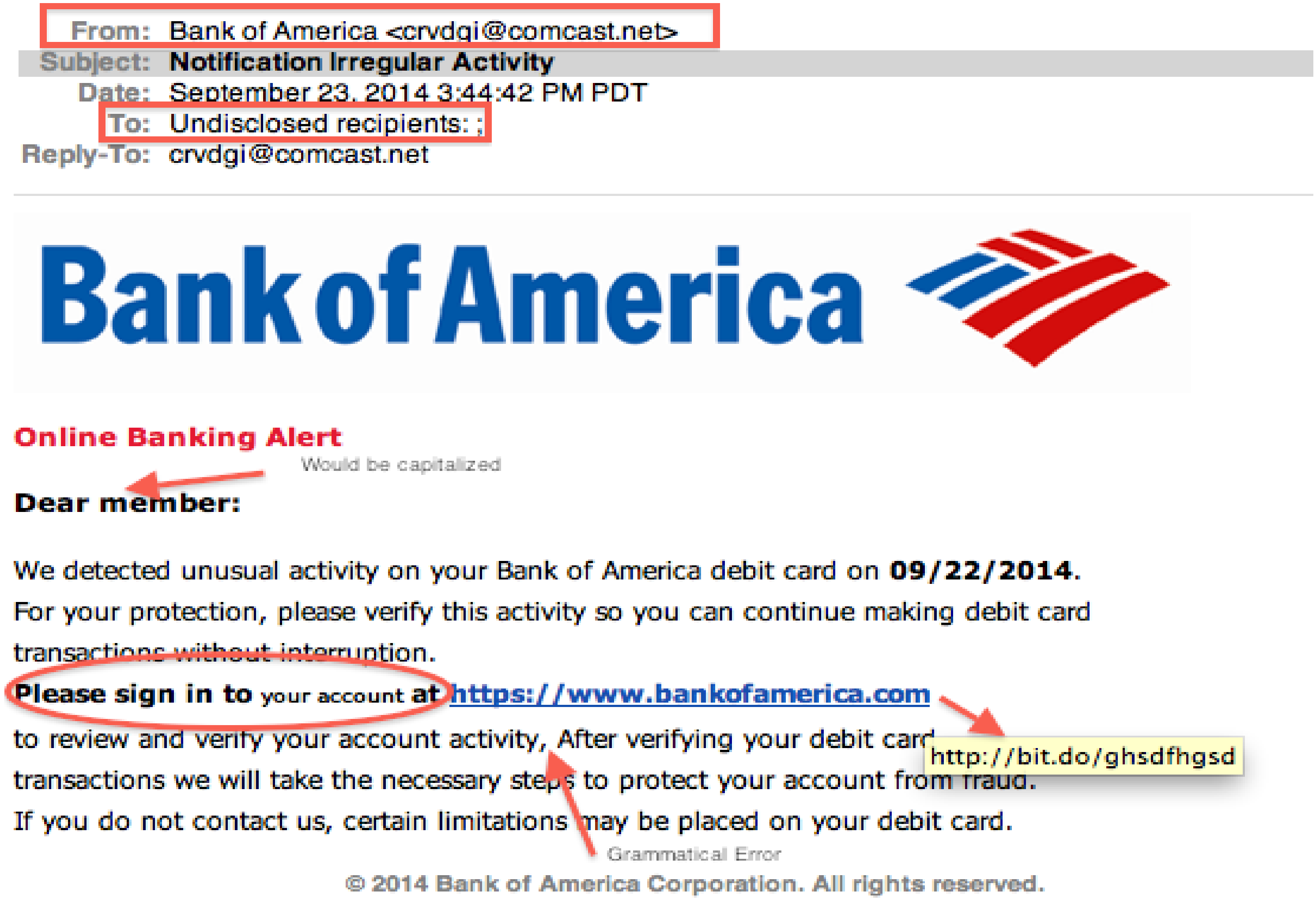
Your password reset is in process and your current password will be disable shortly the password reset link will be forward to the new optional email submitted

Ignore this email notification your request will take effect shortly

If you did not request this password reset
Use Cancel Request button to cancel the password reset and keep your

This action will take a brief period before this request takes effect
This is a mandatory communication about the service. To set communication preferences for other cases.

PHISHING – HOW TO DETECT



From: Bank of America <crvdgi@comcast.net>
Subject: **Notification Irregular Activity**
Date: September 23, 2014 3:44:42 PM PDT
To: Undisclosed recipients: ;
Reply-To: crvdgi@comcast.net

Online Banking Alert

Would be capitalized

Dear member:

We detected unusual activity on your Bank of America debit card on **09/22/2014**. For your protection, please verify this activity so you can continue making debit card transactions without interruption.

Please sign in to your account **at** https://www.bankofamerica.com

http://bit.do/ghsdfhgsd

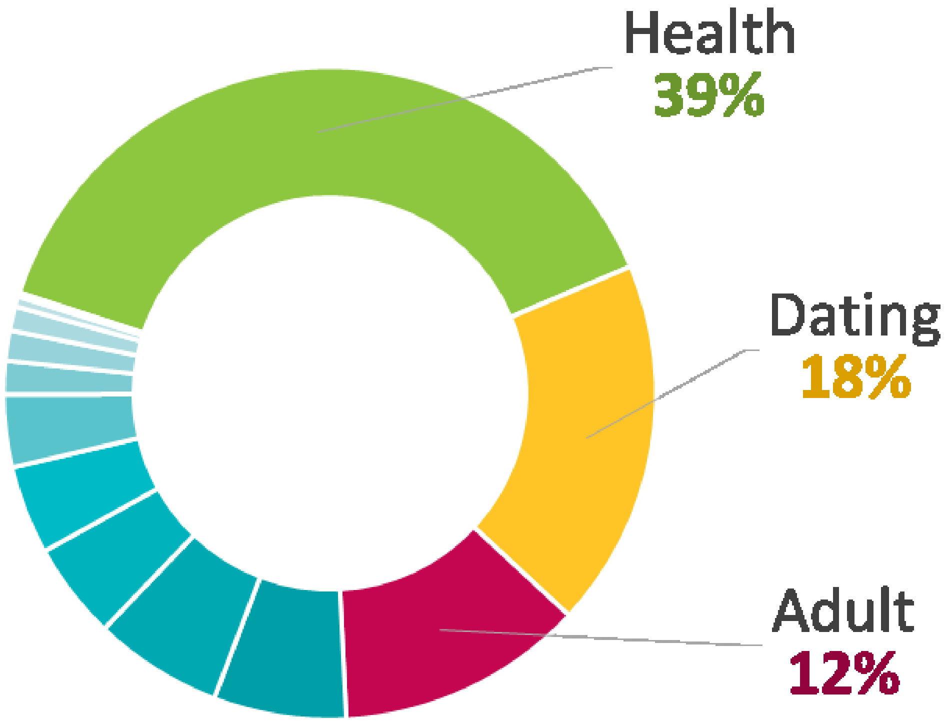
to review and verify your account activity, After verifying your debit card transactions we will take the necessary steps to protect your account from fraud. If you do not contact us, certain limitations may be placed on your debit card.

Grammatical Error

© 2014 Bank of America Corporation. All rights reserved.

PHISHING STATS

- 54% of all inbound em spam
- 1 in 20 email message malicious content



PHISHING STATS

30% of people

Open phishing messages (23% last year)

12% of people

Open attachments (11% last year)

TOP TIPS TO AVOID PHISHING

1. Check who the email sender is.
2. Check the email for grammar and spelling mistakes.
3. Mouse over the link to see where it goes.
4. Do not click the link – manually type it in.

THREATS OVERVIEW

Social Engineering

SOCIAL ENGINEERING

- The most effective way to crack through a companies defenses
- Non-technical intrusion that relies on human interaction and often involves tricking people into **breaking the rules**
- It’s a way of hacking the human

SOCIAL ENGINEERING EXAMPLE

- In one of the IT Labs one person enters in a rush
- He pretends to have forgotten the password to the UAIC domains and he urgently needs to send a mail to the Dean
- One colleague is willing to help him and logs into with his account to the persons laptop
- Unauthorized person obtained access to the faculty network

TOP TIPS TO AVOID SOCIAL ENGINEERING

1. Be careful with the information you disclose.
2. Verify credentials of contractors.
3. If you have any doubts on the identity of callers, hang up and call their official company number back.

PART 2. GDPR OVERVIEW

GDPR OVERVIEW

- **Main aspects:**
- Personal data
- Breach notification
- Territorial scope

- **Main players**
- Data subject
- Controller
- Processor
- Processing

WHAT IS GDPR?

- **Rules that safeguard the privacy of EU citizens** (data subjects)

- **Who needs to comply?**

Any organization with data on EU individuals, wherever they are based.

- **When does it start?**

GDPR is in effect after 25th May 2018 (so it is already in place) ☺

- **What does this mean?**

Data subjects rights needs to be respected and technical and organizational measures needs to be in place to make sure personal data is safe.

WHAT IS PERSONAL DATA?

- GDPR Defines personal data very broadly:
  “any information relating to an identified or identifiable natural person“

- **Examples:**
  - Name
  - Address
  - Photo
  - Email address
  - Post on social networking websites
  - IP address
  - Bank details
  - Medical information

WHERE IS PERSONAL DATA?

- **Data can be found in:**
  - Customer databases
  - Email content / lists
  - Feedback forms filled out by customers
  - Paper records
  - Photos / CCTV footage
  - Loyalty program records
  - HR / employees database
  - Application or transaction logs
  - Reports on individuals

Stupid joke time:

- Do you know a good GDPR consultant?

- Yes.

- Can you give me his e-mail address?

- No.

DATA SUBJECTS RIGHTS

- **Data Subject / User, owns the data**
- **Explicit rights to:**
  - Access confirmation of existence, logic of automated processing and access to personal data
  - Data portability
  - Correction/rectification
  - Erasure "right to be forgotten"
  - Objection on processing producing legal or significant consequences
  - Restriction of processing for period of time
  - Compensation and liabilities for material or non-material damage

"They had their names removed using the right to be forgotten"

FINE TIME

Up to 4% of global turnover or 20 mln euro, whatever is higher

•Breach of controller or processor obligation

•Breach of data subjects rights and freedoms

•Failure to report the breach

•Breach itself

What can go wrong?

TRUST ME. OUR CLOUD SECURITY IS SO GOOD EVEN YOU WON'T BE ABLE TO ACCESS YOUR DATA!

NOT JUST HACKING

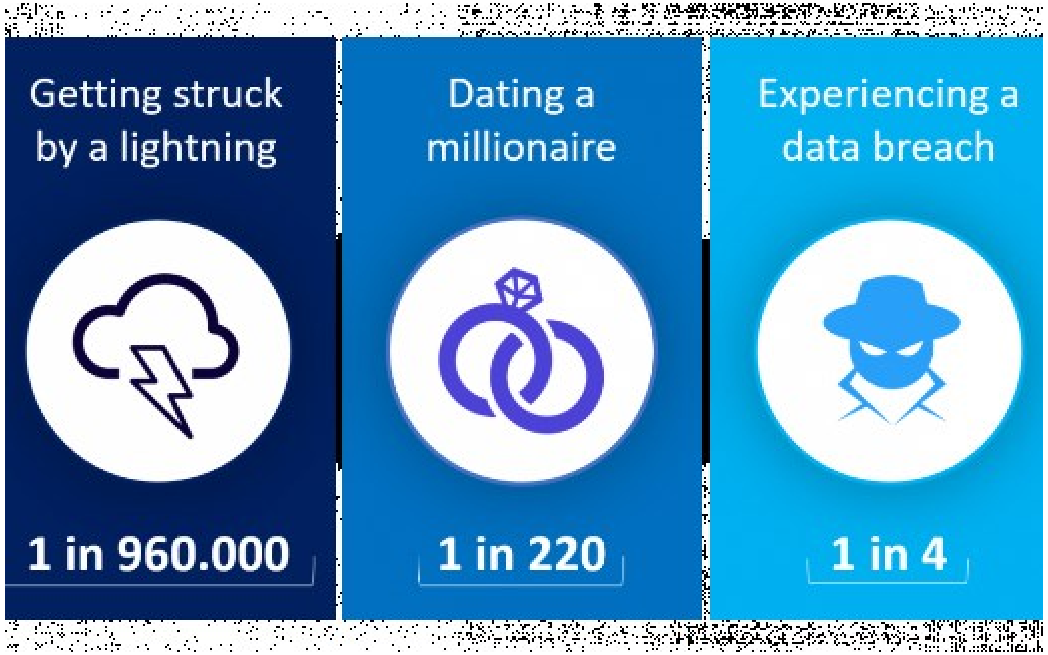
- Inability to meet the deadline for information request.
- Breach of responsibilities of the controller or processor.
- No difference between not-intentional and intentional damage.

06 by Randy Glasbergen.
gen.com

“The identity I stole was a fake!
Boy, you just can’t trust people these days!”

EXAMPLES OF BREACHES

- **Security Incidents:**
- Password compromised
- Confidential information exposed on Internet
- Lost badge / laptop
- Stolen / lost on call mobile phone with company e-mails



- **Data breaches:**
- Data leak / loss or theft of information
- Deleted data accidentally or on purpose
- Personal data transferred to wrong receiver

- Need to be reported as soon as possible after detection!

PART 2. ARCHITECTURE OF PRIVACY

ARCHITECTURE OF PRIVACY – MAIN POINTS

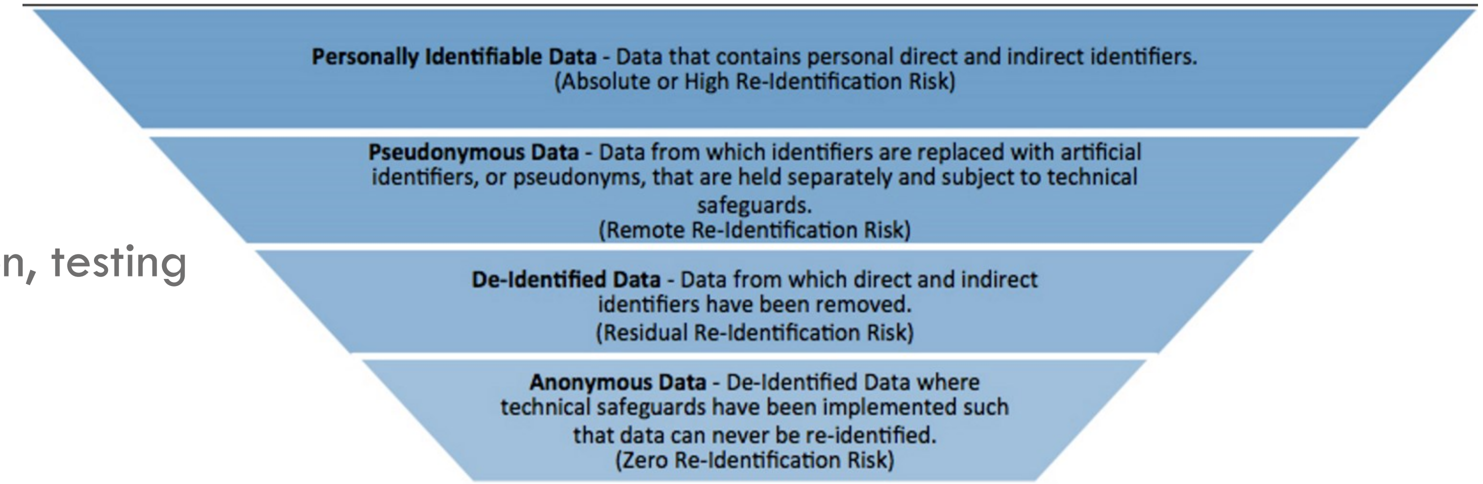
- Private data minimization
- Anonymisation and pseudo-anonymisation
- Data Encryption
- Data Retention
- Security, Integrity and Confidentiality

PRIVATE DATA MINIMIZATION

- Collect only minimal data necessary for processing/service
- Remove fields not needed
- Remove records not needed
- Don’t log personal data
- Handle backups and restores
- Production/Test/Development/Analytics …

ANONYMISATION AND PSEUDO-ANONYMISATION

- **Pseudonymization** is a method to substitute identifiable data with a reversible, consistent value.
- **Anonymization** is the destruction of the identifiable data.
- **Anonymised data**
  - Not subject of GDPR
  - Not so easy to perform properly
  - Useful for statistics and aggregation, testing
- **Pseudonymized data**
  - Subject of GDPR
  - Keep key mappings safe (best on the controller side)
  - Generally can be used all around including production systems



Personally Identifiable Data - Data that contains personal direct and indirect identifiers. (Absolute or High Re-Identification Risk)

Pseudonymous Data - Data from which identifiers are replaced with artificial identifiers, or pseudonyms, that are held separately and subject to technical safeguards. (Remote Re-Identification Risk)

De-Identified Data - Data from which direct and indirect identifiers have been removed. (Residual Re-Identification Risk)

Anonymous Data - De-Identified Data where technical safeguards have been implemented such that data can never be re-identified. (Zero Re-Identification Risk)

DATA ENCRYPTION

- Not mandatory by GDPR
  - But good idea anyway
  - As good as your key management
- If/when things go wrong – best ticket out
  - Breach notification of data subjects not mandatory
  - Considered as cornerstone of responsible data handling
- Applicable on
  - Data in transit (communication protocols, APIs, emails…)
  - Data at rest (storage level, databases, tables, records..)
  - Backups, VMs. AMIs…
  - Personal hardware devices (e.g. laptops, mobiles, USB and external disks…)

DATA RETENTION

Don’t keep data for longer than necessary for specific purpose/consent

- Periodically (automatically) remove expired data or data not needed
- Keep audit log of activities.
- Don’t forget on backups, VMs, test data …
- Full anonymisation of data is same as deleting (from GDPR perspective)

Retention period

- Data subject consent (campaign participation, newsletter consent)
- Processing/contract justification
- Legal justification
- Don’t forget restore points of backup.

Consent

SECURITY, INTEGRITY AND CONFIDENTIALITY

- General rules, best practices and industry standards applies
- GDPR prescribes risk based approach The measures should ensure an appropriate level of security, including confidentiality, taking into account the state of the art and the costs of implementation in relation to the risks and the nature of the personal data to be protected.
- GDPR does not prescribe any specific technology or process
- In absence of GDPR standardisation and certification ISO 27001 considered next best thing for showing compliance.
- Integrity and confidentiality are equally important GDPR Personal data Breach is breach of security leading to the accidental or unlawful **destruction**, **loss**, **alteration**, unauthorized **disclosure** of, or **access** to, personal data transmitted, stored or otherwise processed;

SECURE DEVELOPMENT

- Secure Development Environment
  - Understand the tools and the frameworks used
  - Do not store passwords in any Code Repository
  - Never share property code or config files over the Interr
- Security in the software development lifecycle
  - Following the industry accepted security best practices
  - OWASP Top Ten
- System security testing
- Code review by the peer / pull requests

OWASP

Open Web Application
Security Project

GO TO HTTPS://KAHOOT.IT AND ENTER PIN

Q&A

levi nine

Technology Services