Information Security Awareness

APPS
Information Communication Technology

Who are we?

IT company provides range of Information technology services

Business Solutions

- ERP Solution

[illegible]

[illegible]

- Mobile Applications Development

[illegible]

IT Security Solutions and Services

Solutions:
- SIEM
- SOAR
- UEBA
- UTM

Services:
- Vulnerability Assessment
- Penetration Testing
- IT Security Policy Development
- Security Training and Awareness

Countermeasures
People
Technology
Process
CyberCrime
Cyber-Bullying
Cyber-Extortion
Information Security
Threat
Vulnerability
Risk
Mitigation
Agenda
Preface
Information Security
CyberSecurity Threats
Countermeasures
CyberCrime
Thank You
Preface
2020

Information Security Awareness

APPS
Information Communication Technology

Who are we?

IT company provides range of Information technology services

Business Solutions

- ERP Solution

[illegible]

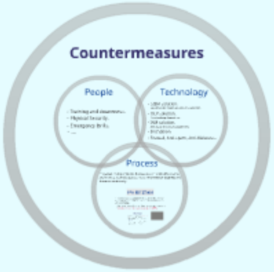
- Mobile Applications Development

[illegible]

IT Security Solutions and Services

Solutions:
- SIEM
- EDRR
- UEBA
- UTM

Services:
- Vulnerability Assessment
- Penetration Testing
- IT Security Policy Development
- Security Training and awareness



Information Security
Threat
Vulnerability
Risk
Mitigation

Agenda

- Preface
- Information Security
- CyberSecurity Threats
- Countermeasures
- CyberCrime

Thank You

APPS

Information Communication Technology

Who are we?

IT company provides range of Information technology services

Business Solutions

- ERP Solution

Integrated systems, Scalable designs to meet the current and future business requirements.

HR Systems, Financial Systems, Payroll, Inventory/Stock Control, Purchase Orders, Purchasing, Sale Orders, Invoicing, Point Of Sales, Statistical Analysis, Marketing, Manufacturing and thousand of other business related systems.

- Mobile Applications Development

Our expert development team works on the cutting edge of technology and best practices.

IT Security Solutions and Services

Solutions:

- SIEM
- SOAR
- UEBA
- UTM

Services:

- Vulnerability Assessment
- Penetration Testing
- IT Security Policy Development
- Security Training and Awareness

Business Solutions

- ## ERP Solution

Integrated systems, Scalable designs to meet the current and future business requirements.

HR Systems, Financial Systems, Payroll, Inventory/Stock Control, Purchase Orders, Purchasing, Sale Orders, Invoicing, Point Of Sales, Statistical Analysis, Marketing, Manufacturing and thousand of other business related systems.

- ## Mobile Applications Development

Our expert development team works on the cutting edge of technology and best practices.

IT Security Solutions and Services

Solutions:

- SIEM
- SOAR
- UEBA
- UTM

Services:

- Vulnerability Assessment
- Penetration Testing
- IT Security Policy Development
- Security Training and Awareness

Information Security Awareness

APPS
Information Communication Technology

Who are we?

IT company provides range of Information technology services

Business Solutions

- ERP Solution

[illegible]

- Mobile Applications Development

[illegible]

IT Security Solutions and Services

Solutions:

- SIEM
- EDRR
- UEBA
- UTM

Services:

- Vulnerability Assessment
- Penetration Testing
- IT Security Policy Development
- Security Training and Awareness

Countermeasures

People

- Training and awareness
- Physical Security
- Emergency Drills
- ...

Technology

Process

CyberCrime

Cyber-Bullying

Cyber-Extortion

Information Security

Threat

Vulnerability

Risk

Mitigation

Agenda

- Preface
- Information Security
- CyberSecurity Threats
- Countermeasures
- CyberCrime

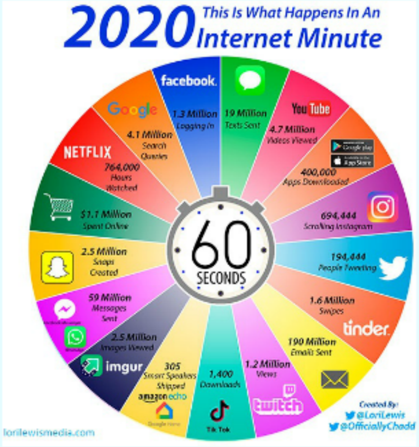
Thank You

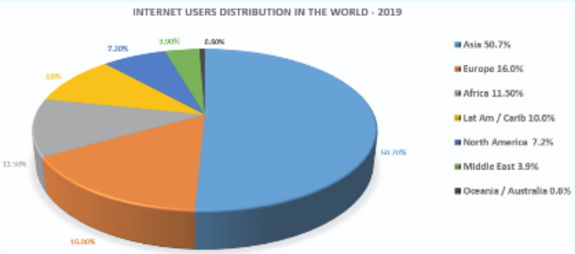
Preface

Agenda

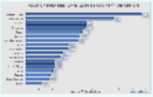
- Preface
- Information Security
- CyberSecurity Threats
- Countermeasures
- CyberCrime

Preface





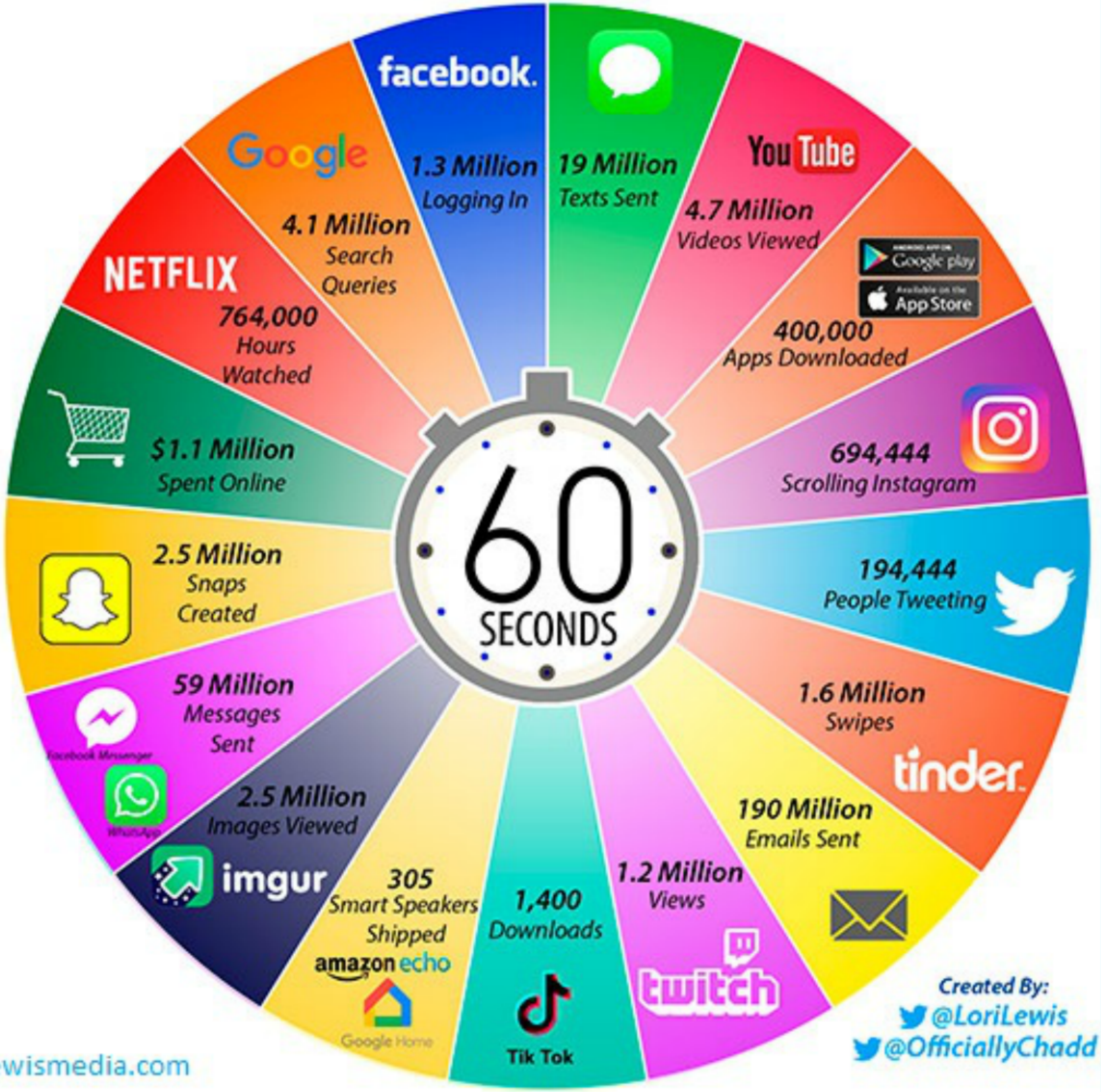
Cyber-Attacks Statistics



Hackers attack every 39 Seconds

CyberAttacks 2019-2020

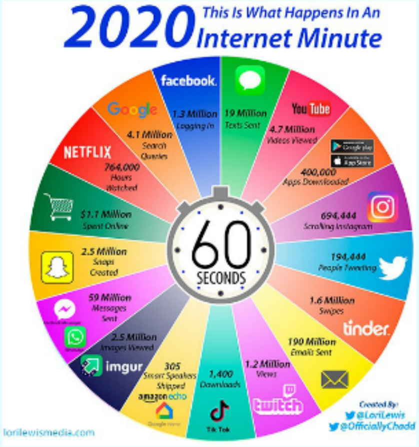
2020 This Is What Happens In An Internet Minute

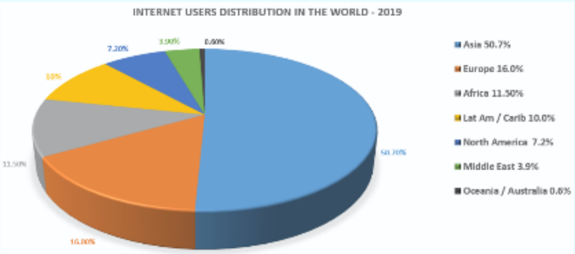


lorilewismedia.com

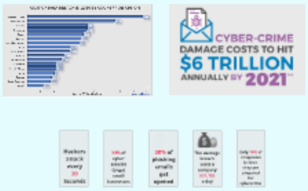
Created By:
@LoriLewis
@OfficiallyChadd

Preface

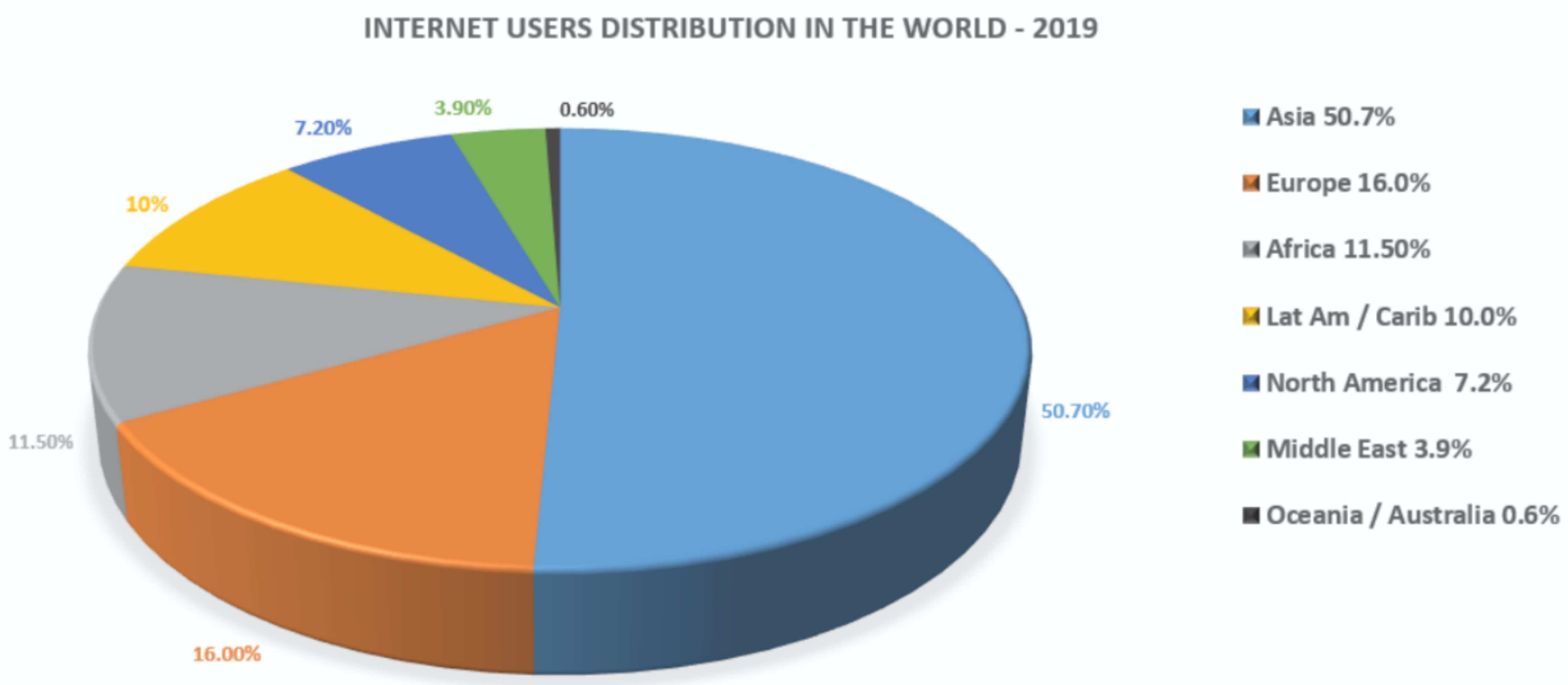




Cyber-Attacks Statistics

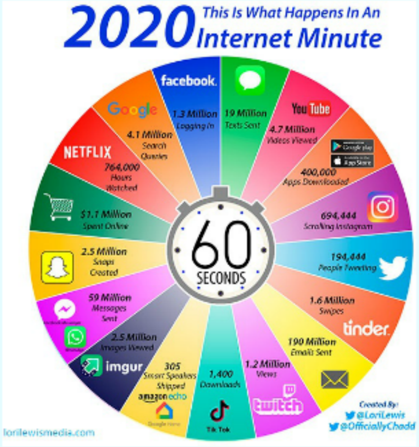


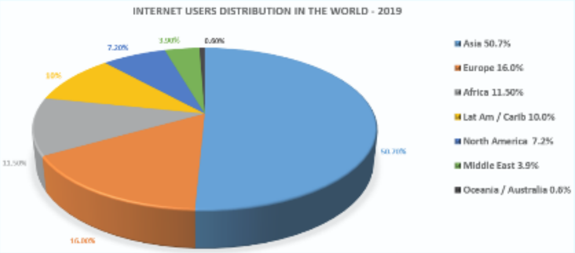
CyberAttacks 2019-2020



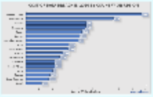
INTERNET USERS DISTRIBUTION IN THE WORLD - 2019

Preface



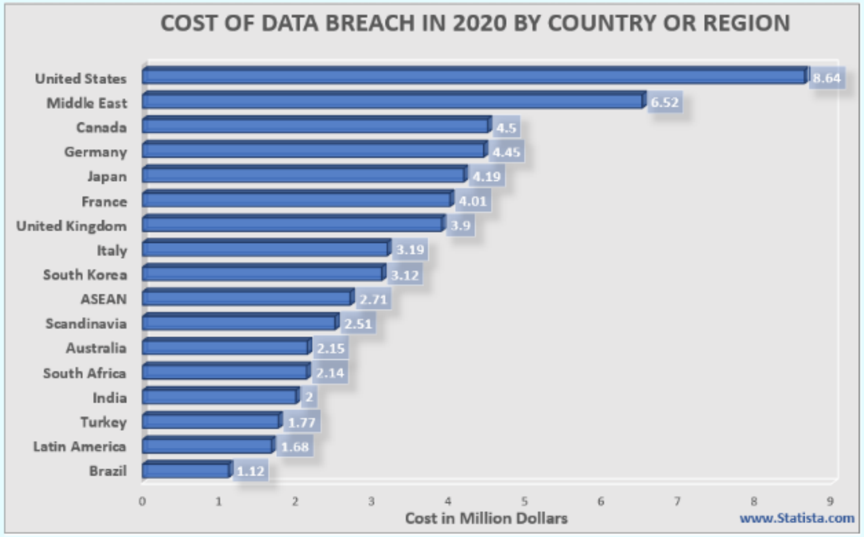


Cyber-Attacks Statistics



CyberAttacks 2019-2020

Cyber-Attacks Statistics



COST OF DATA BREACH IN 2020 BY COUNTRY OR REGION

www.Statista.com

CYBER-CRIME DAMAGE COSTS TO HIT **$6 TRILLION** ANNUALLY BY **2021****

Hackers attack every **39** Seconds

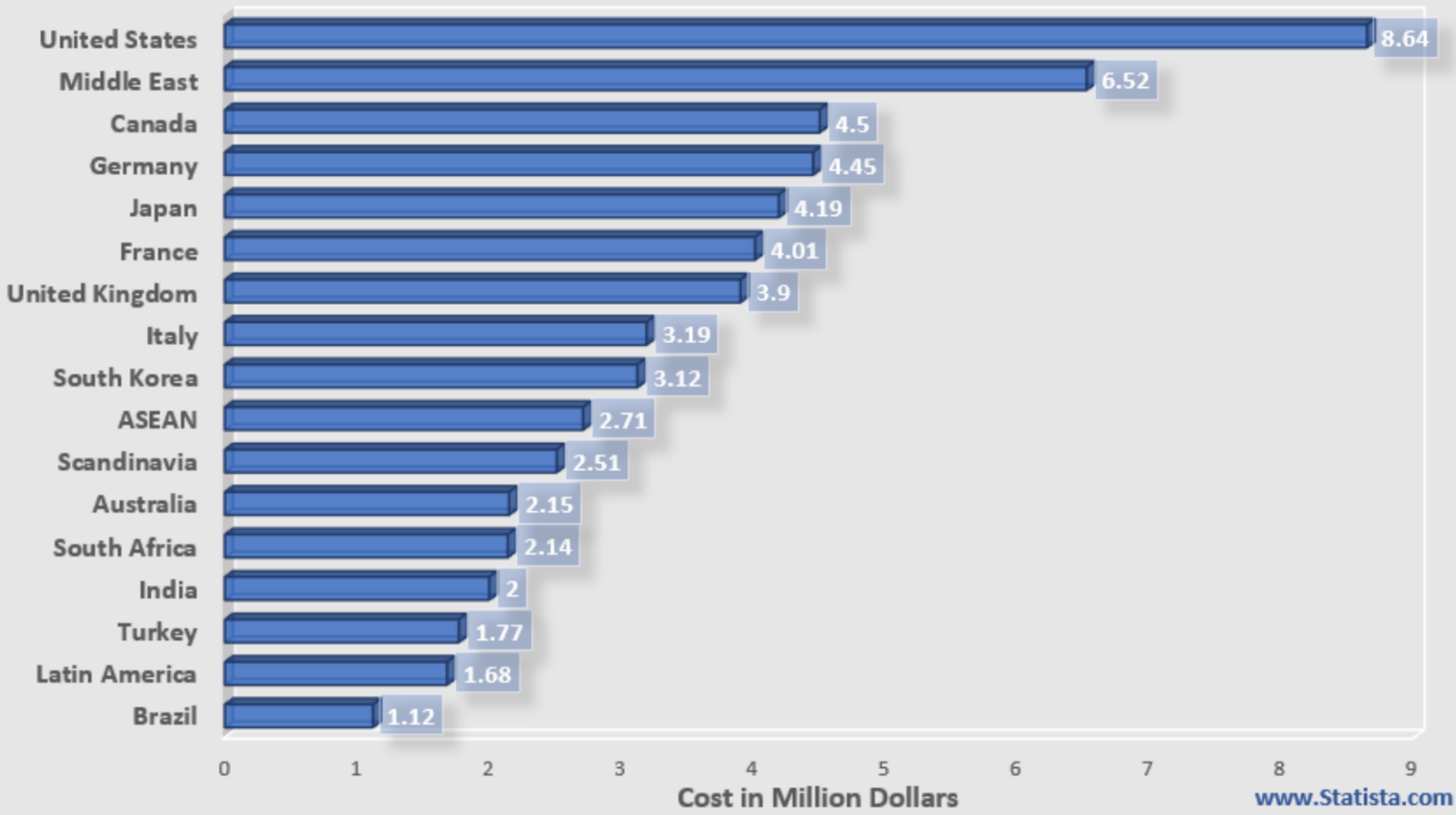
34% of cyber attacks target small businesses

30% of phishing emails get opened

The average breach costs a company **$21,155** a day

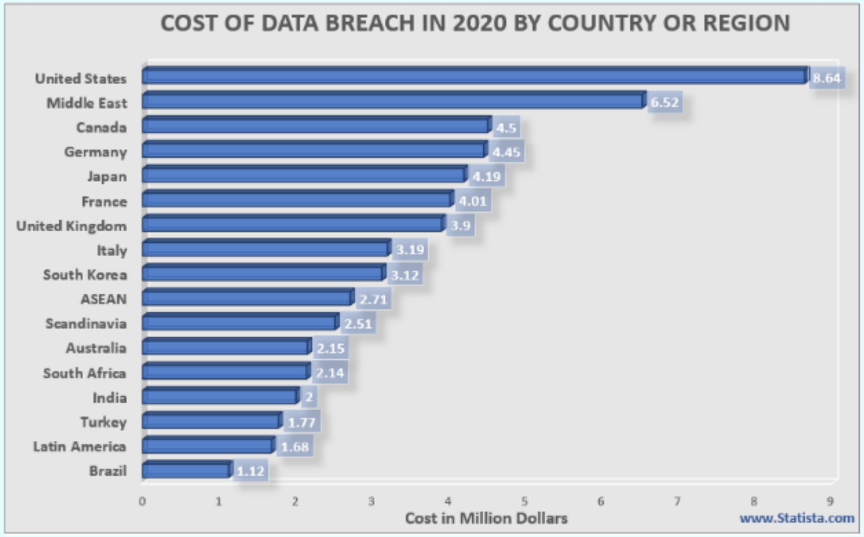
Only **14%** of companies believe they are prepared for cybercrime

COST OF DATA BREACH IN 2020 BY COUNTRY OR REGION



www.Statista.com

Cyber-Attacks Statistics



CYBER-CRIME DAMAGE COSTS TO HIT $6 TRILLION ANNUALLY BY 2021**

Hackers attack every 39 Seconds

34% of cyber attacks target small businesses

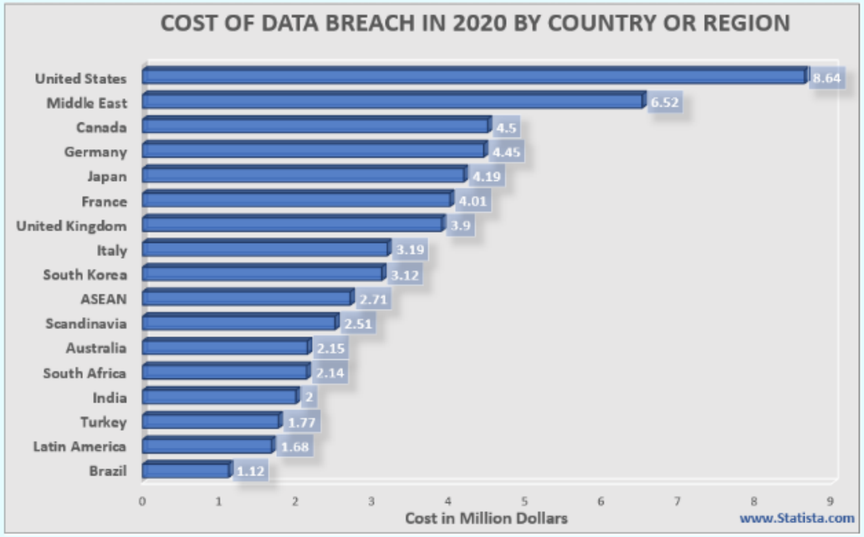
30% of phishing emails get opened

The average breach costs a company $21,155 a day

Only 14% of companies believe they are prepared for cybercrime

CYBER-CRIME DAMAGE COSTS TO HIT $6 TRILLION ANNUALLY BY 2021**

Cyber-Attacks Statistics



CYBER-CRIME DAMAGE COSTS TO HIT **$6 TRILLION** ANNUALLY BY **2021****

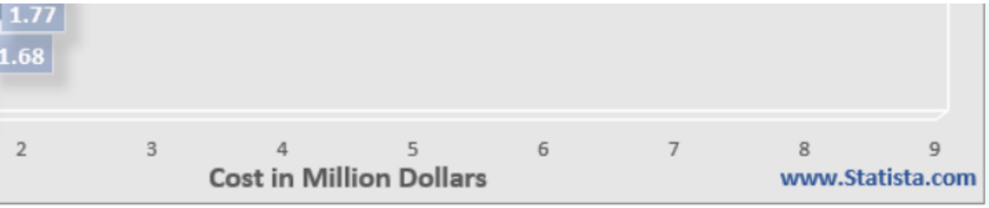
Hackers attack every **39** Seconds

34% of cyber attacks target small businesses

30% of phishing emails get opened

The average breach costs a company **$21,155** a day

Only **14%** of companies believe they are prepared for cybercrime



www.Statista.com

ANNUALLY BY 20

Hackers attack every 39 Seconds

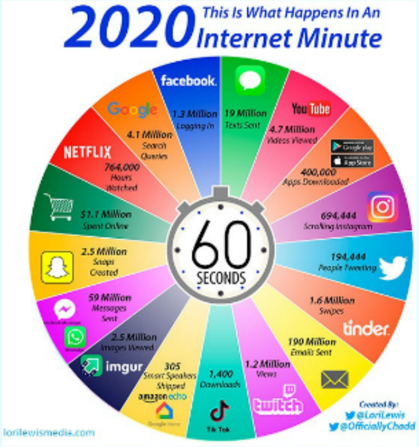
34% of cyber attacks target small businesses

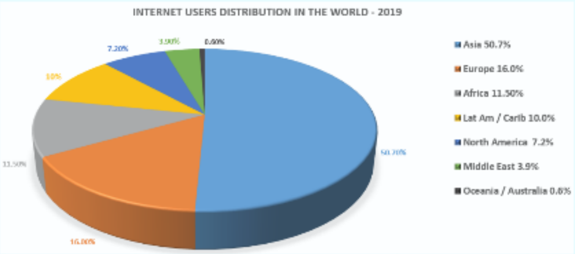
30% of phishing emails get opened

The average breach costs a company $21,155 a day

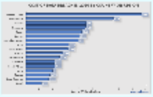
Only 14% of companies believe they are prepared for cybercrime

Preface





Cyber-Attacks Statistics



CYBER-CRIME
DAMAGE COSTS TO HIT
$6 TRILLION
ANNUALLY BY 2021

CyberAttacks 2019-2020

CyberAttacks 2019-2020

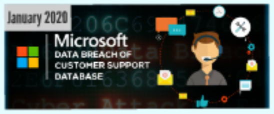
Marriott reveal its second customer data breach in two years.

5.2 Million Guests affected according to CBC News.

Information at risk:

- Addresses
- Dates of birth
- Passport numbers

- The Dutch Donor Register lost external hard drives
- Contain personal data of millions of organ donors
- Includes registrations completed between February 1998 to June 2010



An internal customer support database storing anonymous user analytics became exposed online

They contained 250 million entries

Information at risk:

- Email Addresses
- IP Addresses
- Support case details

- Databases exposed by a criminal group
- 267 million Facebook users infected
- Includes user IDs, names, and phone numbers
- On March 6, 2020 a second server was exposed
- An additional 42 million users infected

Capital One disclosed massive data breach that will cost up to $150M

100M Customers in U.S.	6M Customers in Canada	140K Social security numbers compromised	80K Linked bank accounts compromised

May 2019

aMaDEUS

Leisure Platform

Used by popular Israeli online travel booking services

The leaked database contains:

- International travel plans of the Israeli prime minister, high-ranking Israeli diplomats, and senior agents of Israel's security agencies
  - 36 million booked flights
    - 15 million passengers
      - Over one million hotel bookings
        - 700,000 visa applications

Marriot reveal its second customer data breach in two years.

5.2 Million Guests affected according to CBC News.

Information at risk:

- Addresses
- Dates of birth
- Passport numbers

March 2020

Dutch Government Loses 6.9M Donor Records

- The Dutch Donor Register lost external hard drives
- Contain personal data of millions of organ donors
- Includes registrations completed between February 1998 to June 2010

January 2020

An internal customer support database storing anonymous user analytics became exposed online

They contained 250 million entries

Information at risk:

- Email Addresses
- IP Addresses
- Support case details

December 2019

FACEBOOK DATA BREACH

- Databases exposed by a criminal group
- 267 million Facebook users infected
- Includes user IDs, names, and phone numbers
- On March 6, 2020 a second server was exposed
- An additional 42 million users infected

July 2019

Capital One disclosed massive data breach that will cost up to $150M

100M Customers in U.S.	6M Customers in Canada	140K Social security numbers compromised	80K Linked bank accounts compromised

May 2019

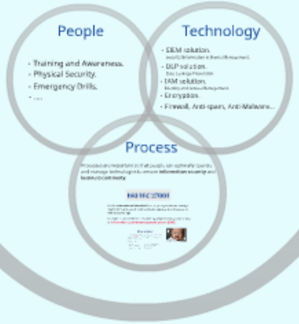
amadeus
Leisure Platform

Used by popular Israeli online travel booking services

The leaked database contains:

- **International travel plans of the Israeli prime minister, high-ranking Israeli diplomats, and senior agents of Israel's security agencies**
- **36 million booked flights**
- **15 million passengers**
- **Over one million hotel bookings**
- **700,000 visa applications**

Countermeasures



People

- Training and Awareness.
- Physical Security.
- Emergency Drills.
- ...

Technology

- SIEM solution.
- DLP solution.
- IAM solution.
- Encryption.
- Firewall, Anti-spam, Anti-Malware...

Process

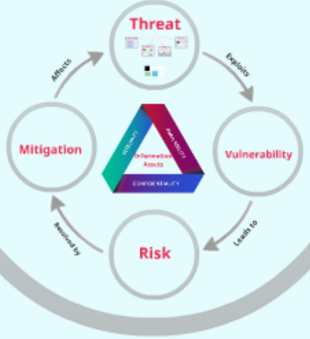
ISO/IEC 27001

CyberCrime

Cyber-Bullying

Cyber-Extortion

Information Security



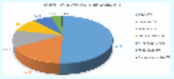
Agenda

- Preface
- Information Security
- CyberSecurity Threats
- Countermeasures
- CyberCrime

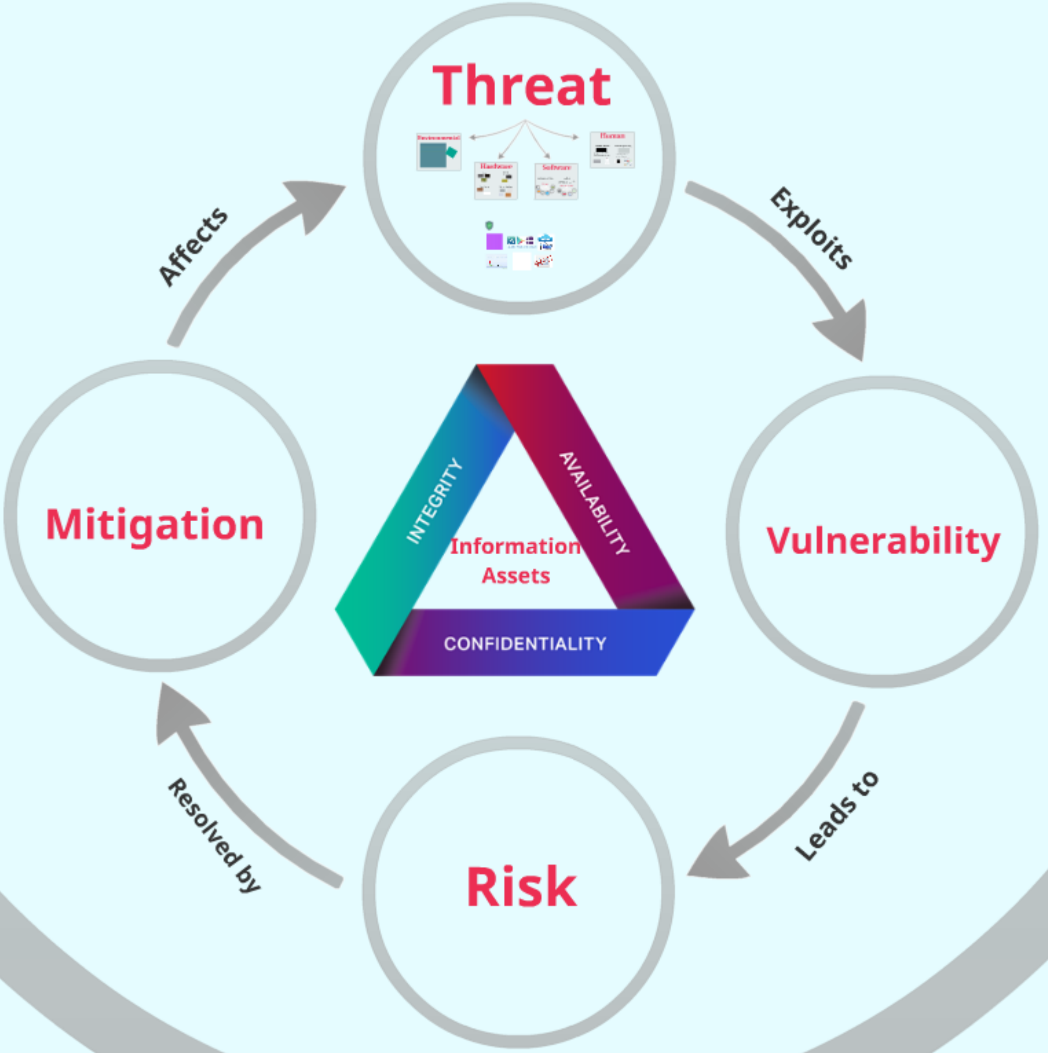
Thank You

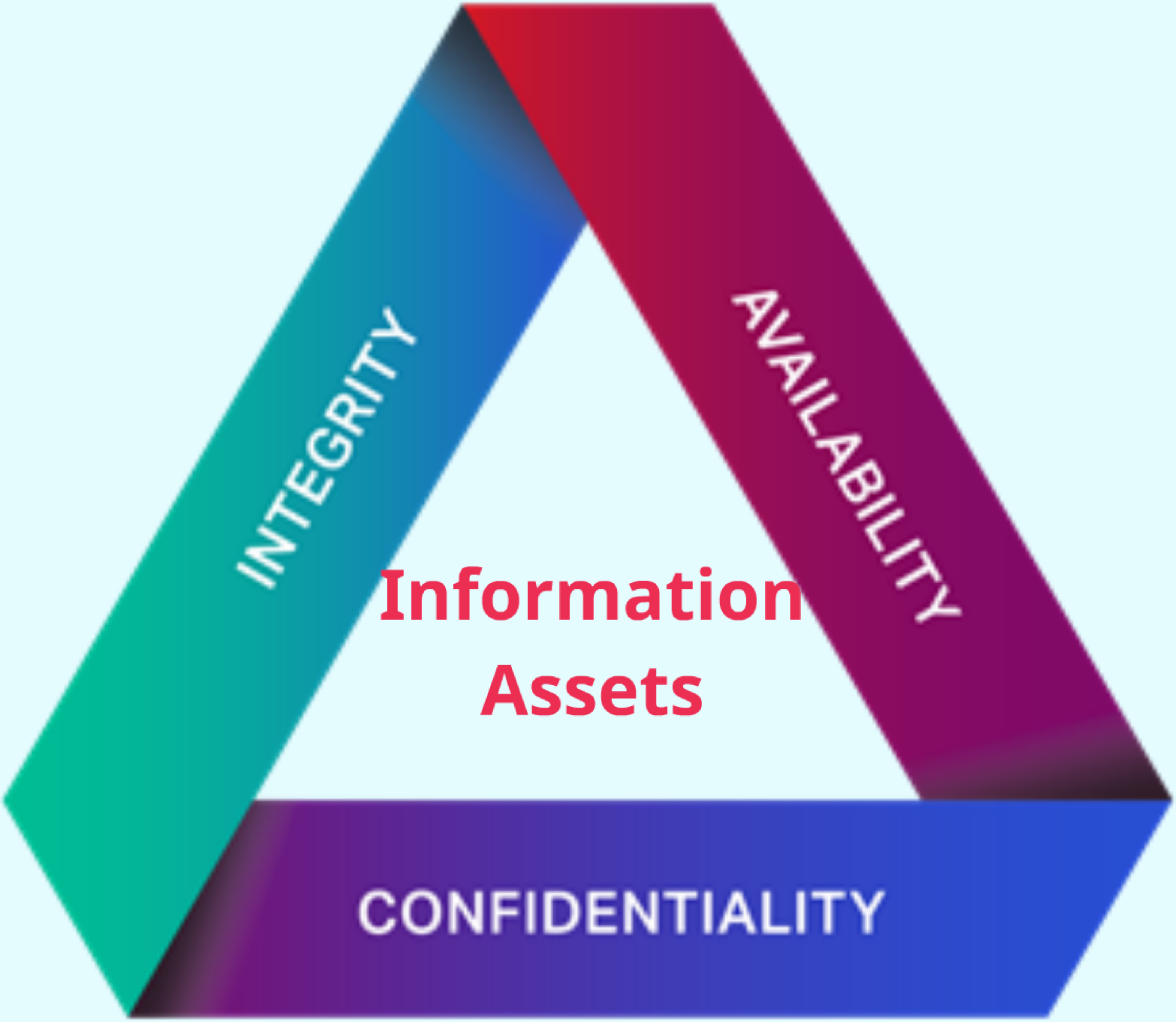
APPS
Information Communication Technology

Preface

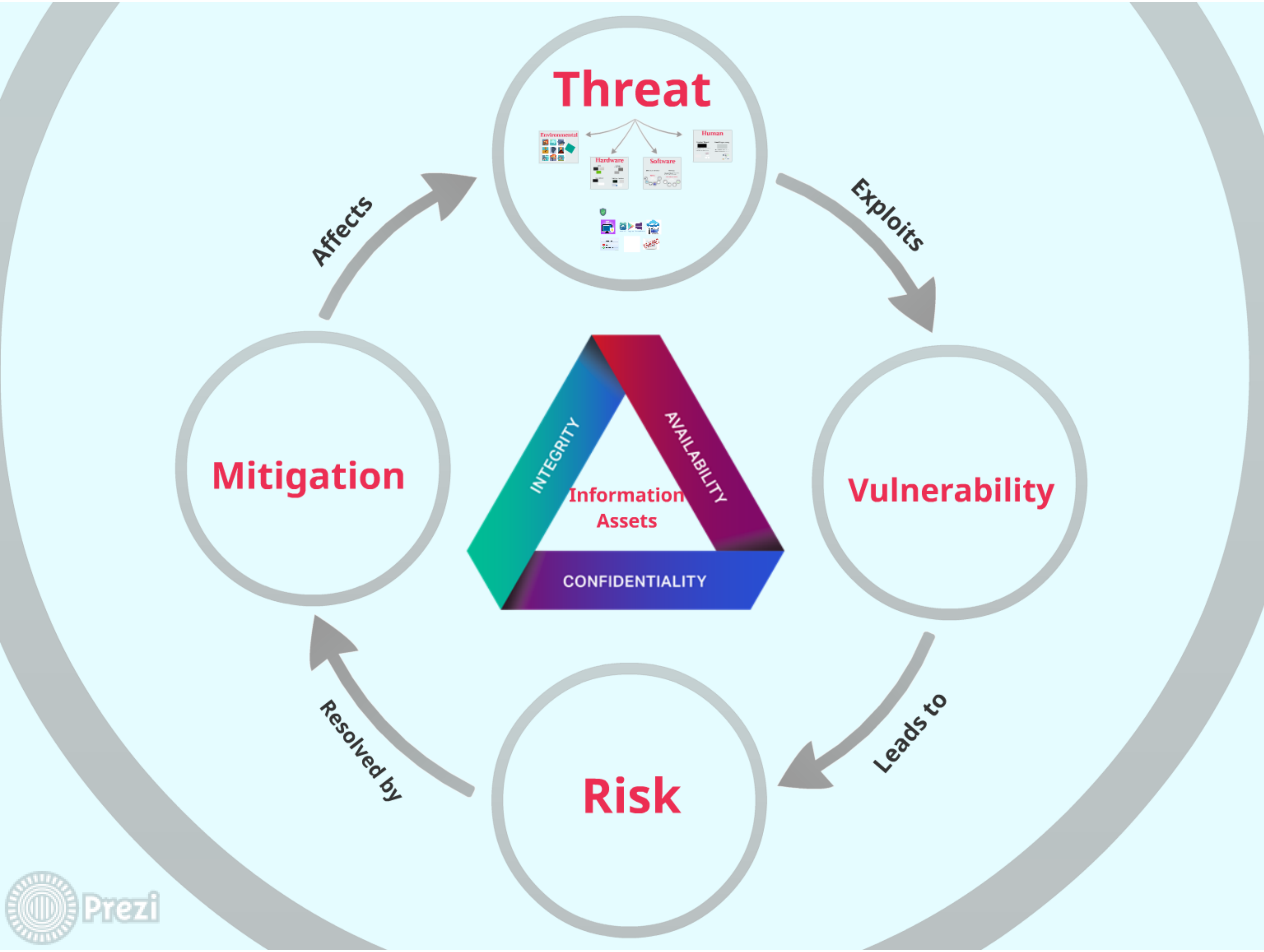


Information Security





Information Assets



Threat

Exploits

Vulnerability

Leads to

Risk

Resolved by

Mitigation

Affects

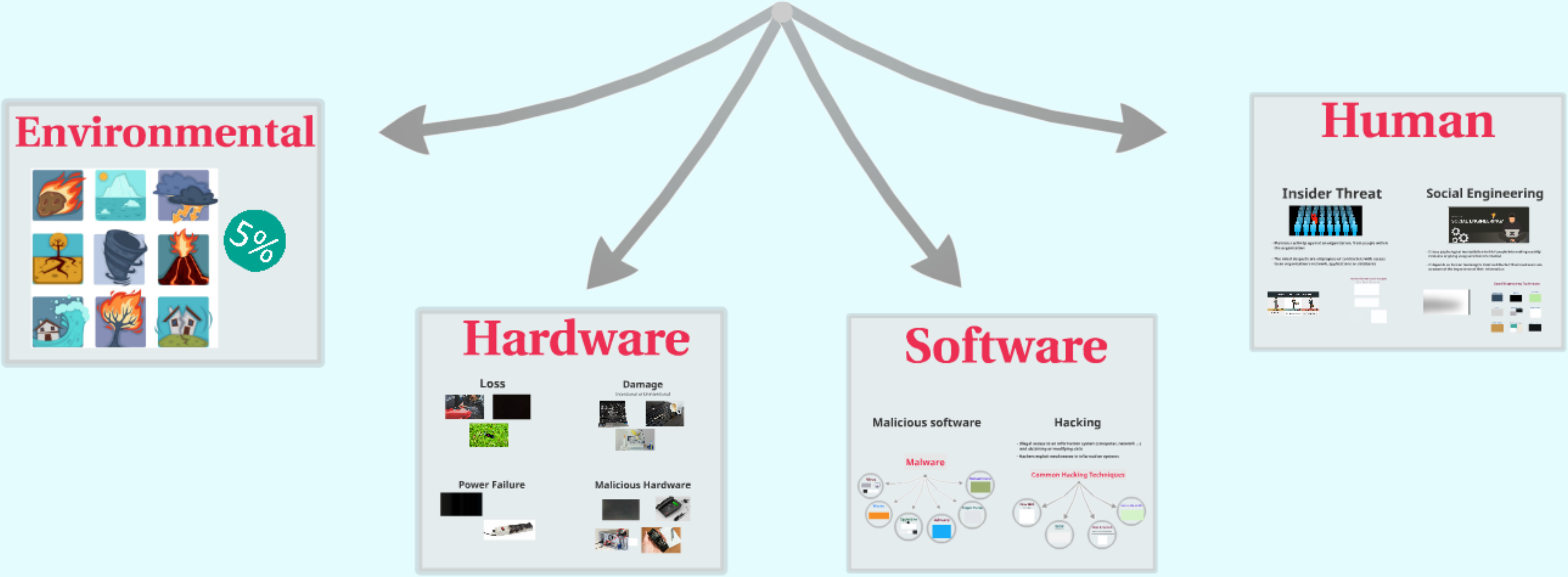
INTEGRITY

AVAILABILITY

CONFIDENTIALITY

Information Assets

Threat



Environmental

Hardware

Loss

Damage

Power Failure

Malicious Hardware

Software

Malicious software

Hacking

Malware

Common Hacking Techniques

Human

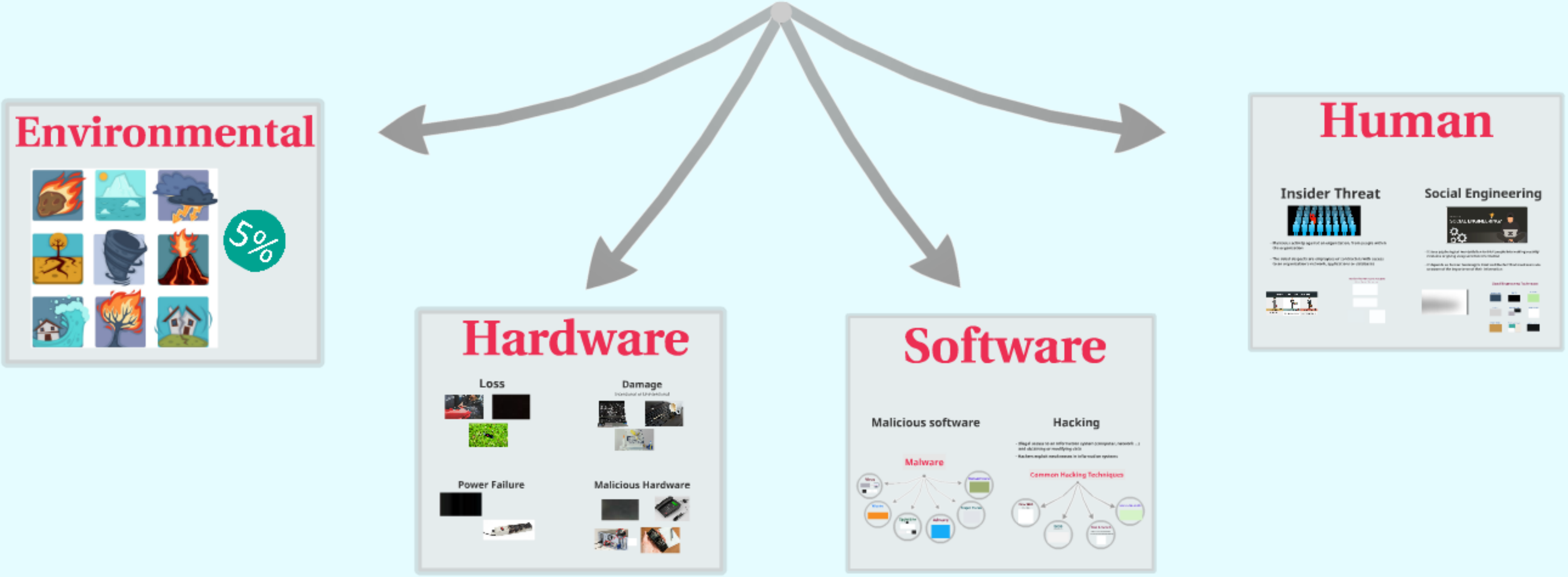
Insider Threat

Social Engineering

Environmental

5%

Threat



Environmental

Hardware

Loss

Damage

Power Failure

Malicious Hardware

Software

Malicious software

Hacking

Malware

Common Hacking Techniques

Human

Insider Threat

Social Engineering

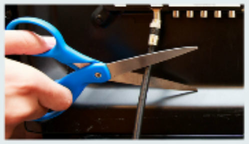
Hardware

Loss

Damage

Intentional or Unintentional

Power Failure



Malicious Hardware

Loss

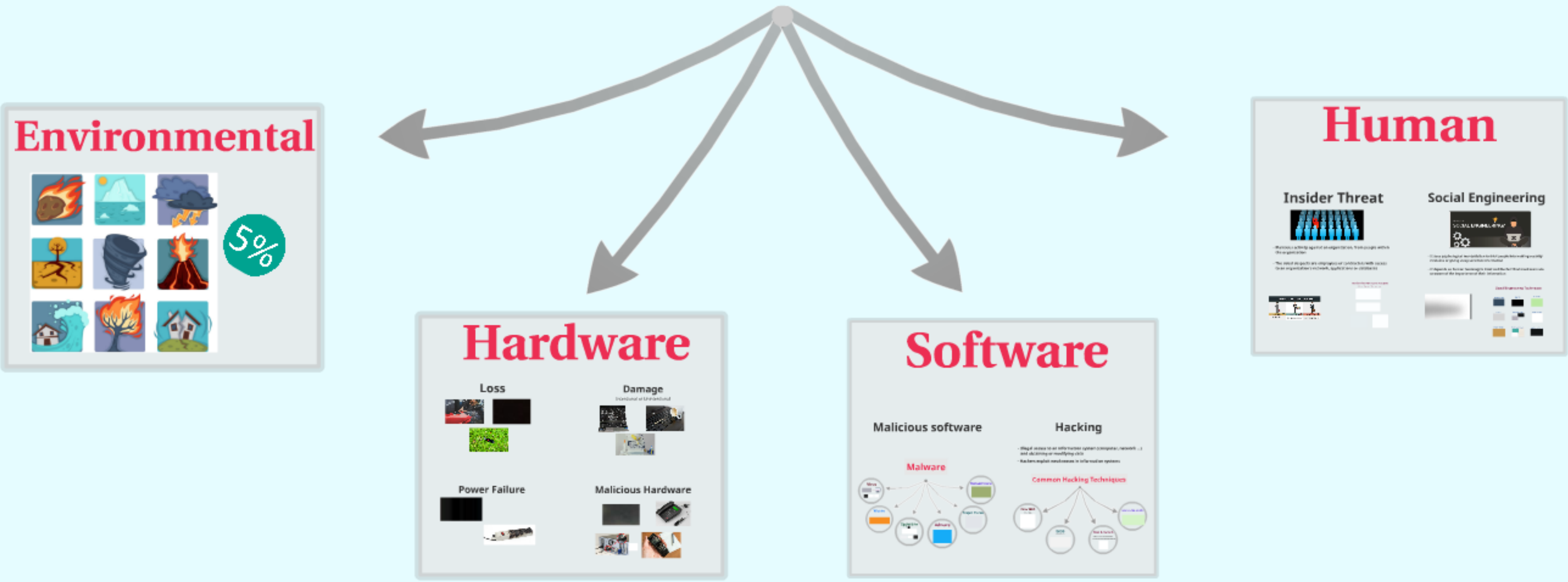
Damage

Intentional or Unintentional

Power Failure

Malicious Hardware

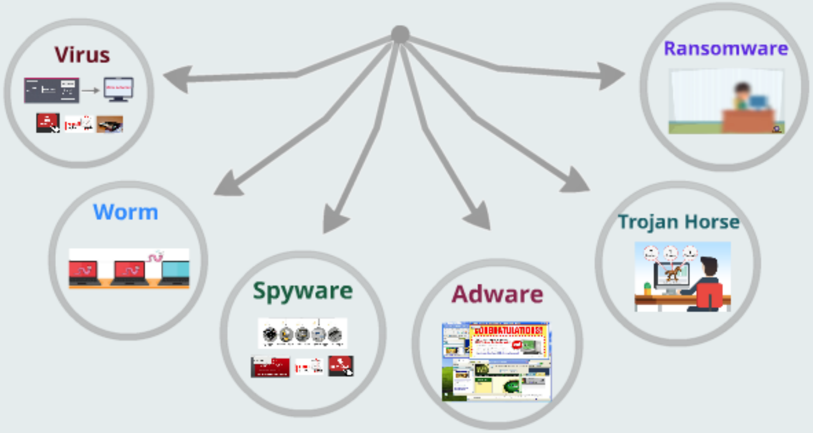
Threat


Environmental
5%
Hardware
Loss
Damage
Power Failure
Malicious Hardware
Software
Malicious software
Malware
Hacking
Common Hacking Techniques
Human
Insider Threat
Social Engineering

Software

Malicious software

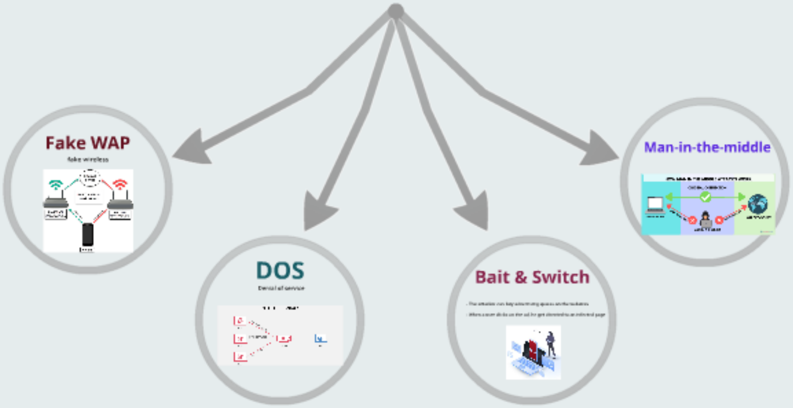
Malware



Hacking

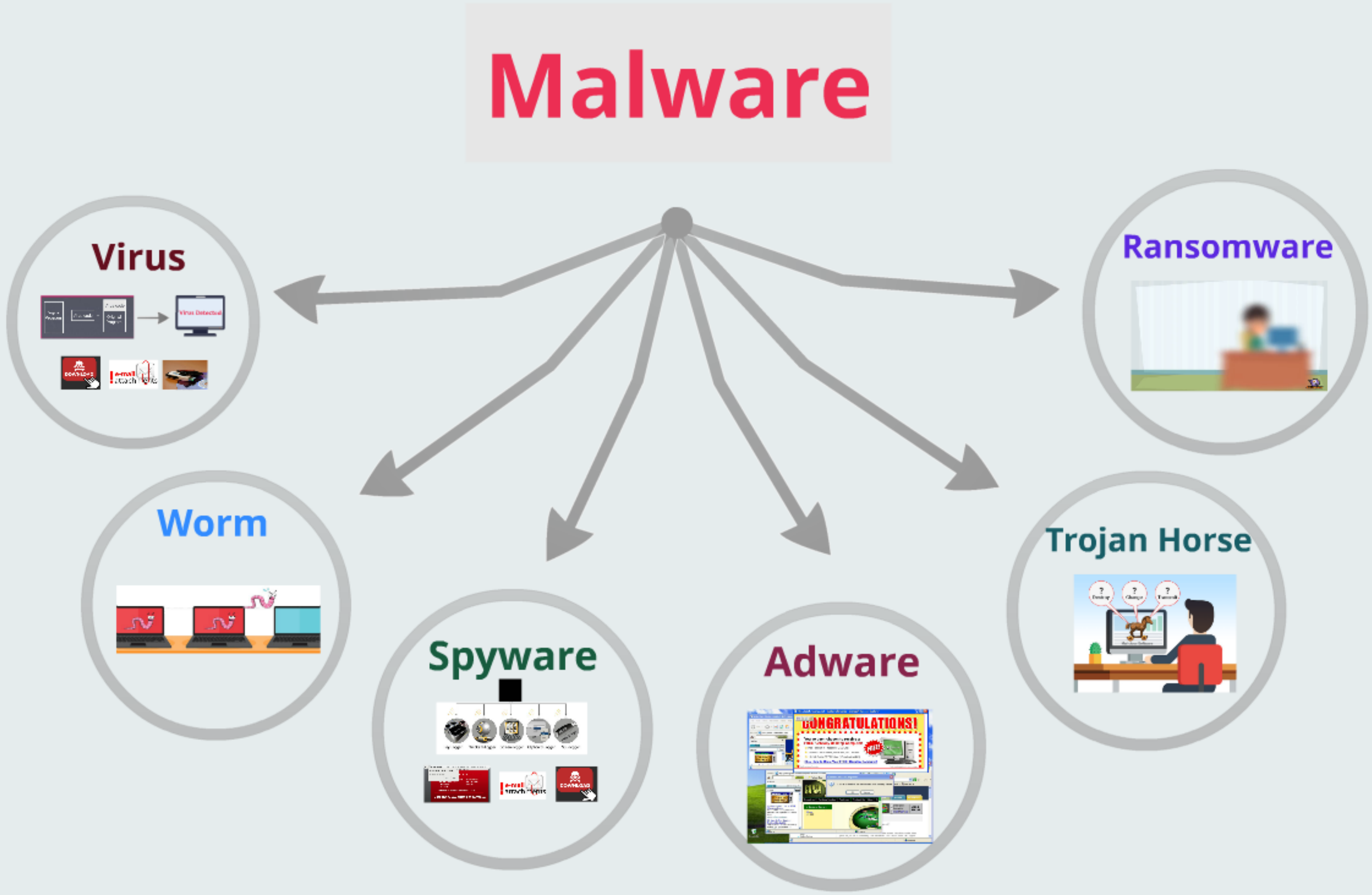
- Illegal access to an information system (computer, network …) and obtaining or modifying data
- Hackers exploit weaknesses in information systems

Common Hacking Techniques



- The attacker can buy advertising spaces on the websites
- When a user clicks on the ad, he get directed to an infected page

Malicious software



Malware

Virus

Worm

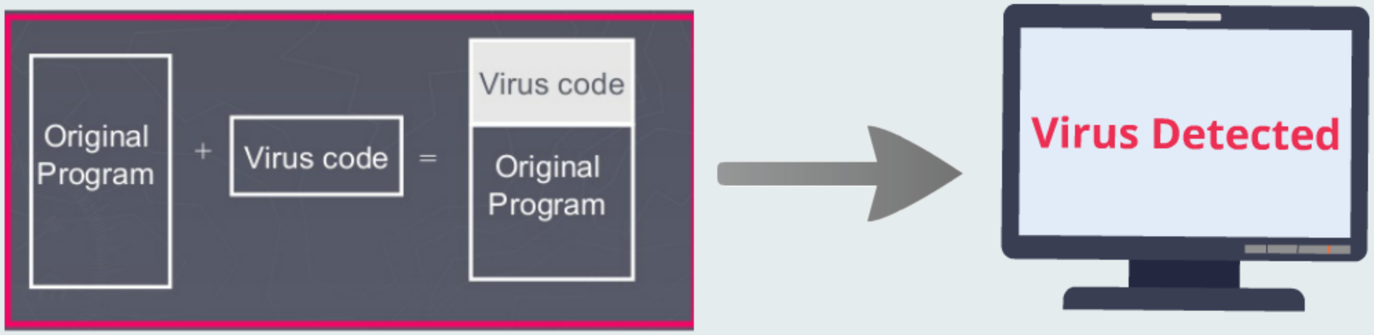
Spyware

Adware

Trojan Horse

Ransomware

Virus

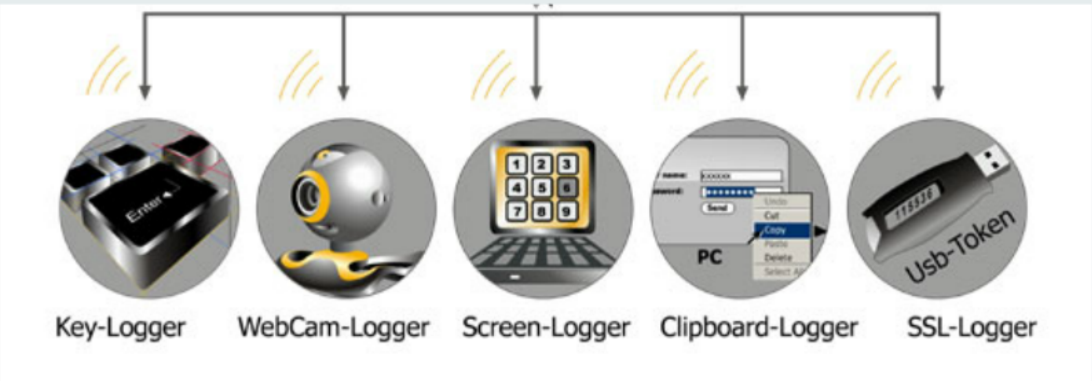

Original Program
+
Virus code
=
Virus code
Original Program
Virus Detected

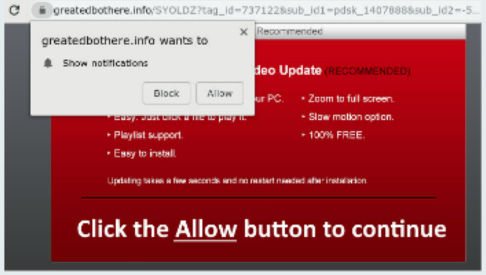
DOWNLOAD

! e-mail attachments

Worm

Spyware




greatedbothere.info/SYOLDZ?tag_id=737122&sub_id1=pdsk_1407888&sub_id2=-5...

greatedbothere.info wants to

Show notifications

Block Allow

Recommended

deo Update (RECOMMENDED)

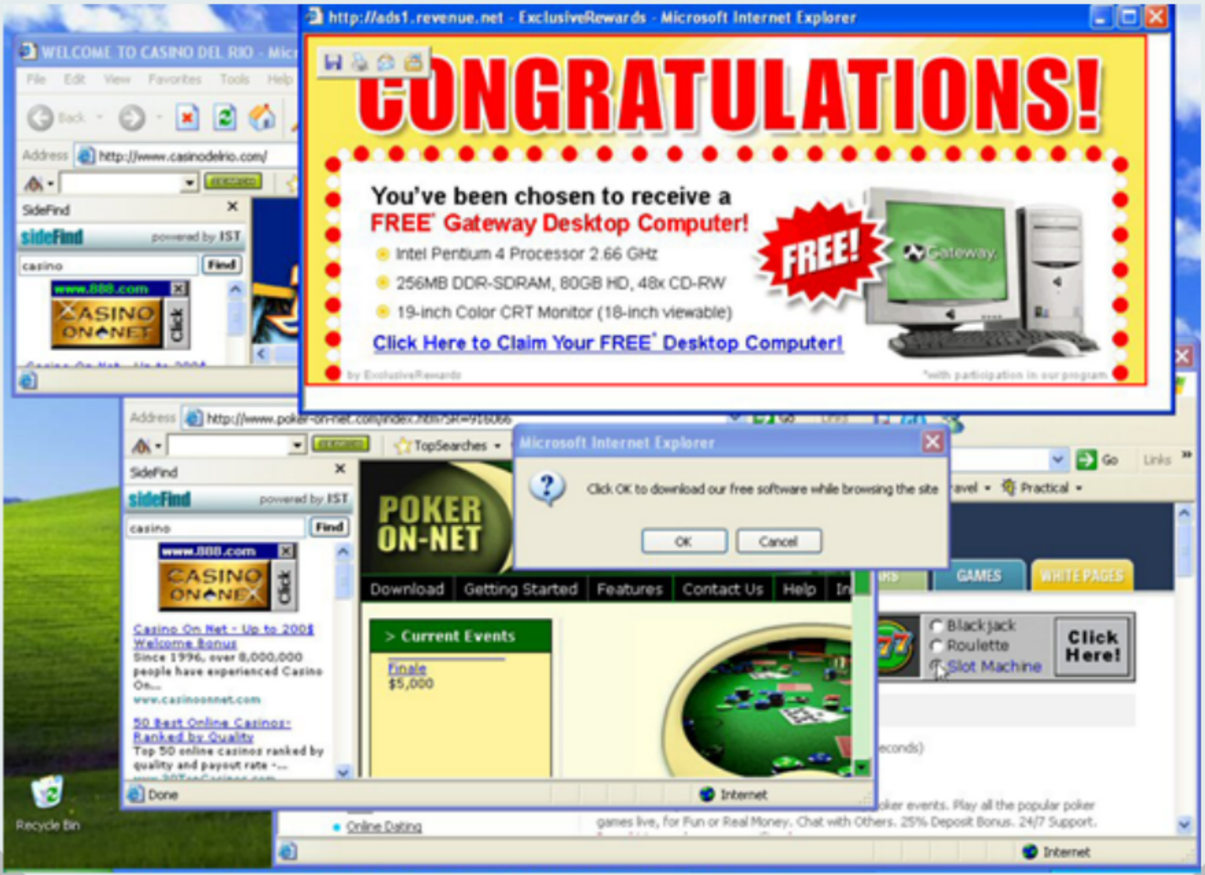
ur PC.

- Easy. Just click a file to play it.
- Playlist support.
- Easy to install.
- Zoom to full screen.
- Slow motion option.
- 100% FREE.

Updating takes a few seconds and no restart needed after installation

Click the Allow button to continue

Adware



CONGRATULATIONS!

You've been chosen to receive a FREE* Gateway Desktop Computer!

- Intel Pentium 4 Processor 2.66 GHz
- 256MB DDR-SDRAM, 80GB HD, 48x CD-RW
- 19-inch Color CRT Monitor (18-inch viewable)

Click Here to Claim Your FREE* Desktop Computer!

FREE!

by ExclusiveRewards

*with participation in our program

Microsoft Internet Explorer

Click OK to download our free software while browsing the site

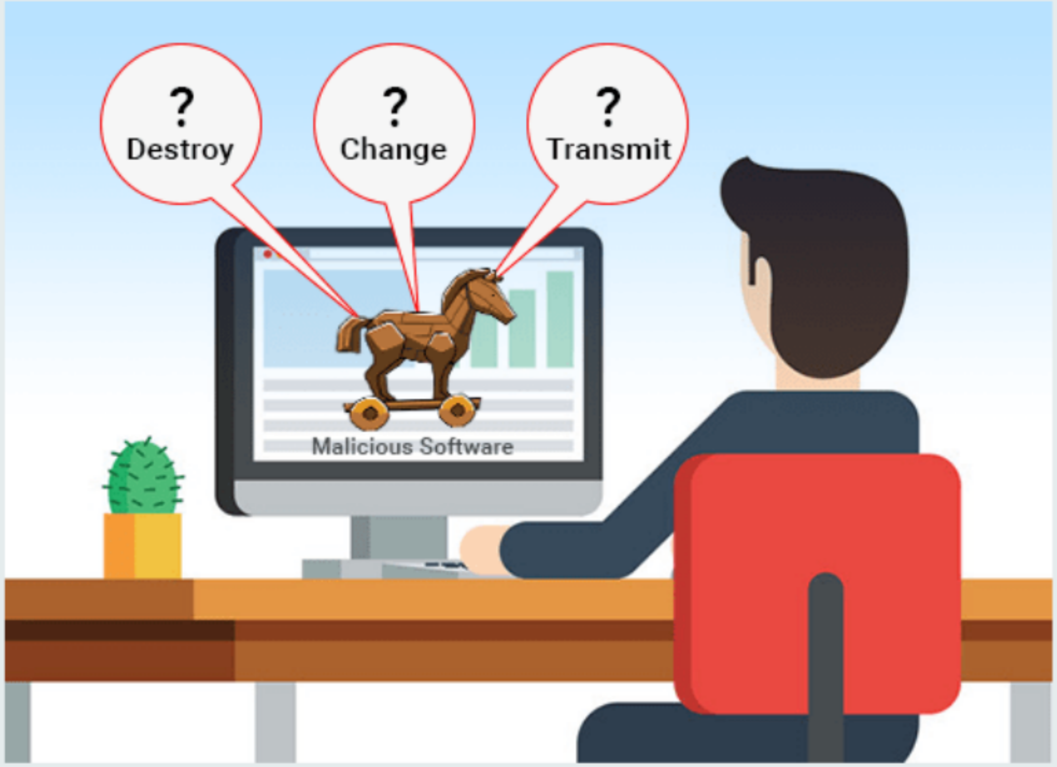
OK Cancel

Casino On Net - Up to 200$ Welcome Bonus
Since 1996, over 8,000,000 people have experienced Casino On...
www.casinoonnet.com

50 Best Online Casinos: Ranked by Quality
Top 50 online casinos ranked by quality and payout rate -...

...oker events. Play all the popular poker games live, for Fun or Real Money. Chat with Others. 25% Deposit Bonus. 24/7 Support.

Trojan Horse



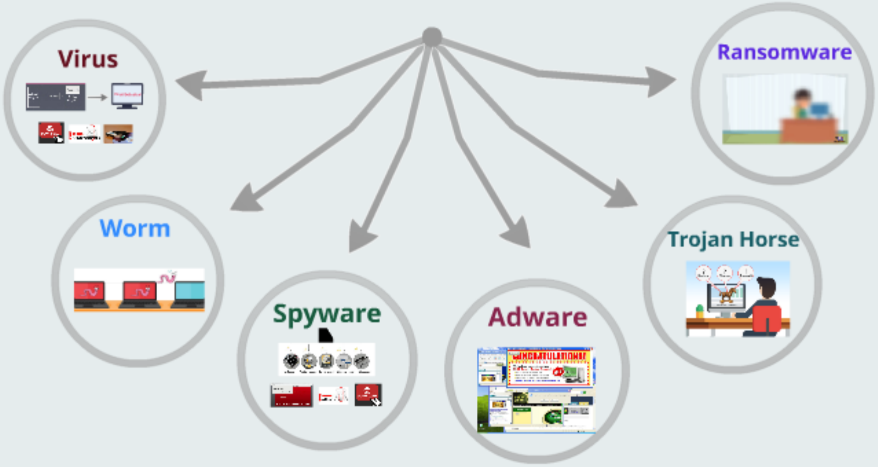
Ransomware

Animaker

Software

Malicious software

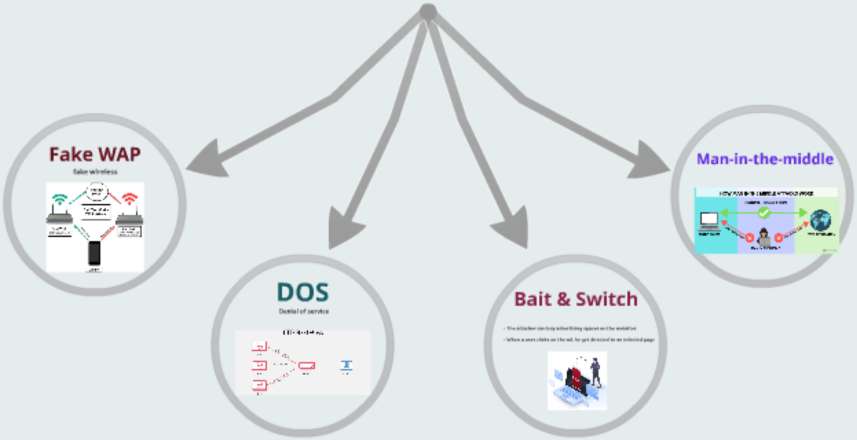
Malware



Hacking

- Illegal access to an information system (computer, network ...) and obtaining or modifying data
- Hackers exploit weaknesses in information systems

Common Hacking Techniques



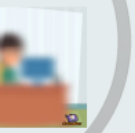
- The attacker can buy advertising spaces on the websites
- When a user clicks on the ad, he get directed to an infected page

Hacking

- Illegal access to an information system (computer, network …) and obtaining or modifying data
- Hackers exploit weaknesses in information systems

Common Hacking Techniques

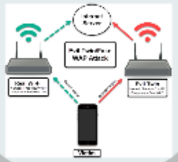
ware



e

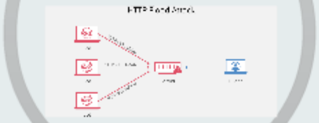
Fake WAP

fake wireless



DOS

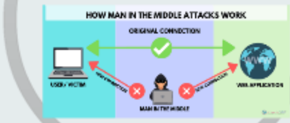
Denial of service



Bait & Switch

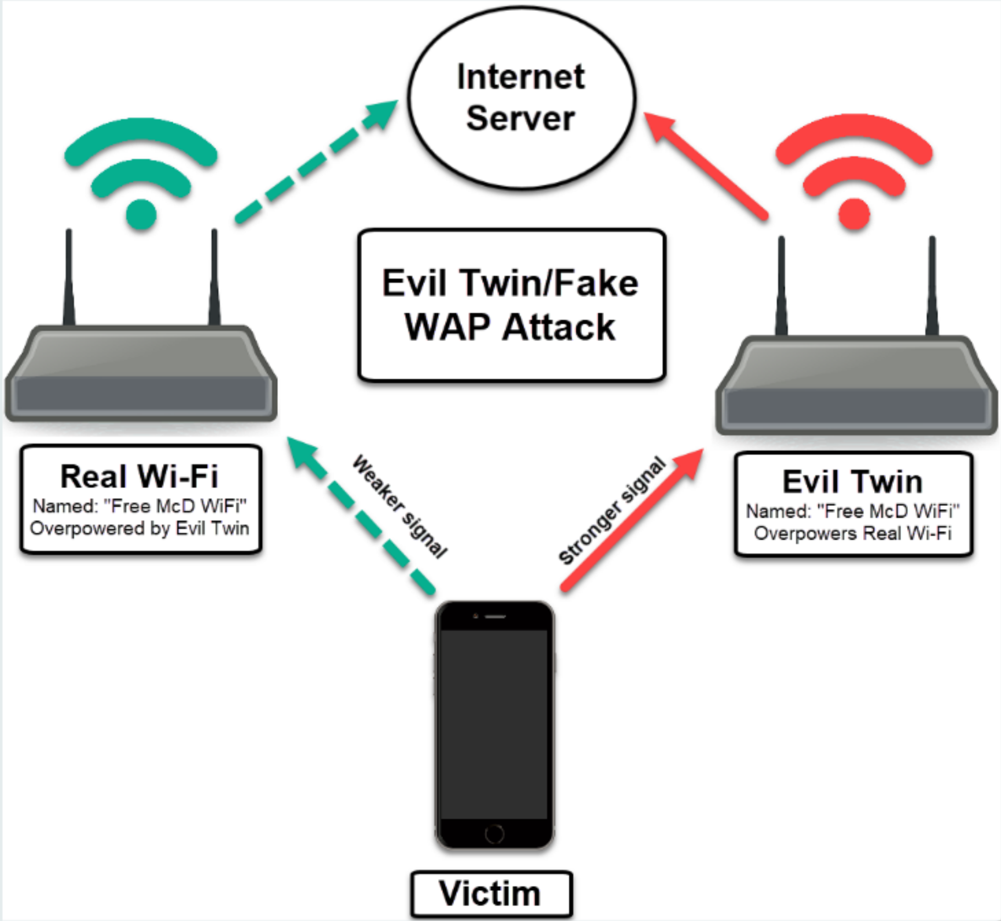
- The attacker can buy advertising spaces on the websites
- When a user clicks on the ad, he get directed to an infected page

Man-in-the-middle



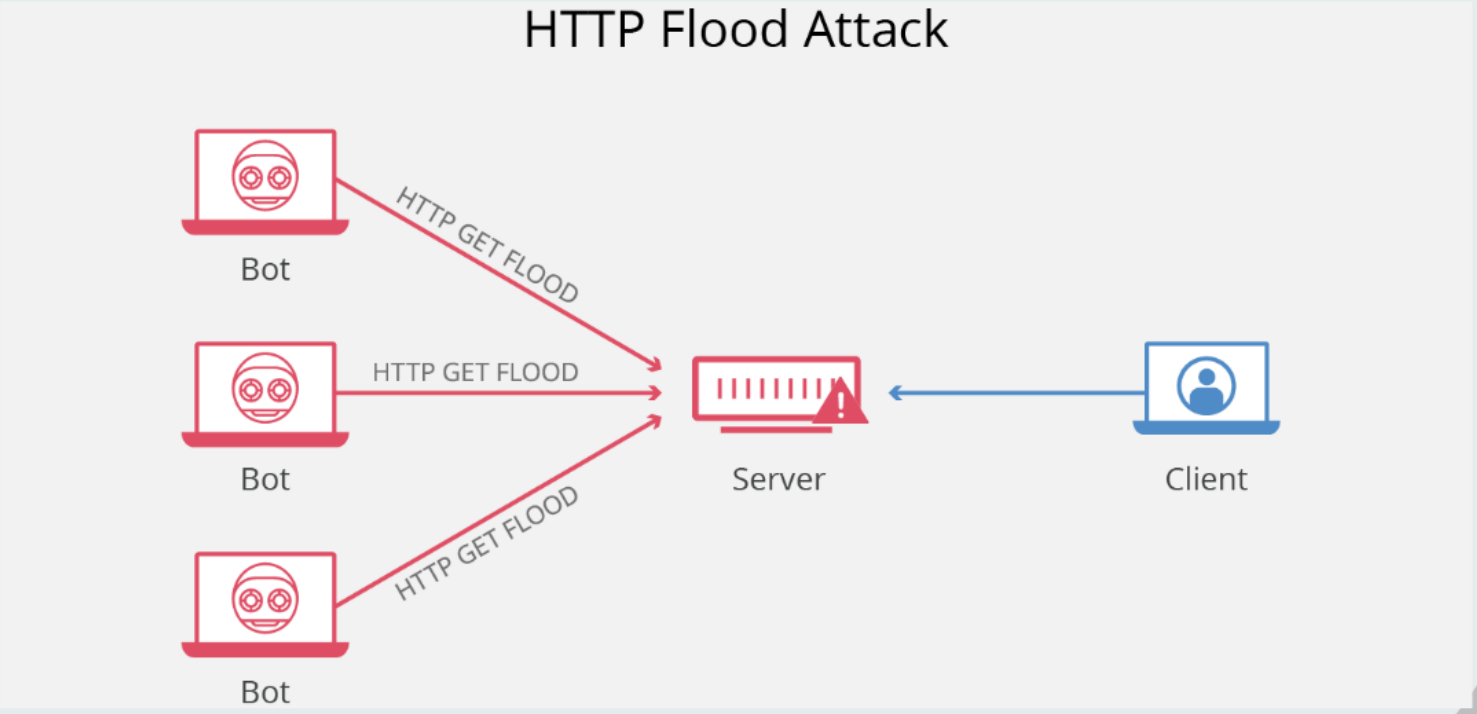
Fake WAP

fake wireless



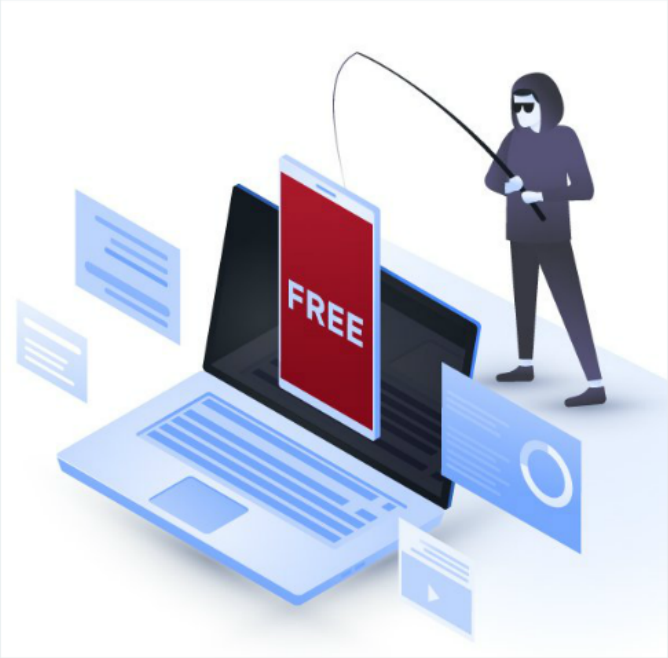
DOS

Denial of service

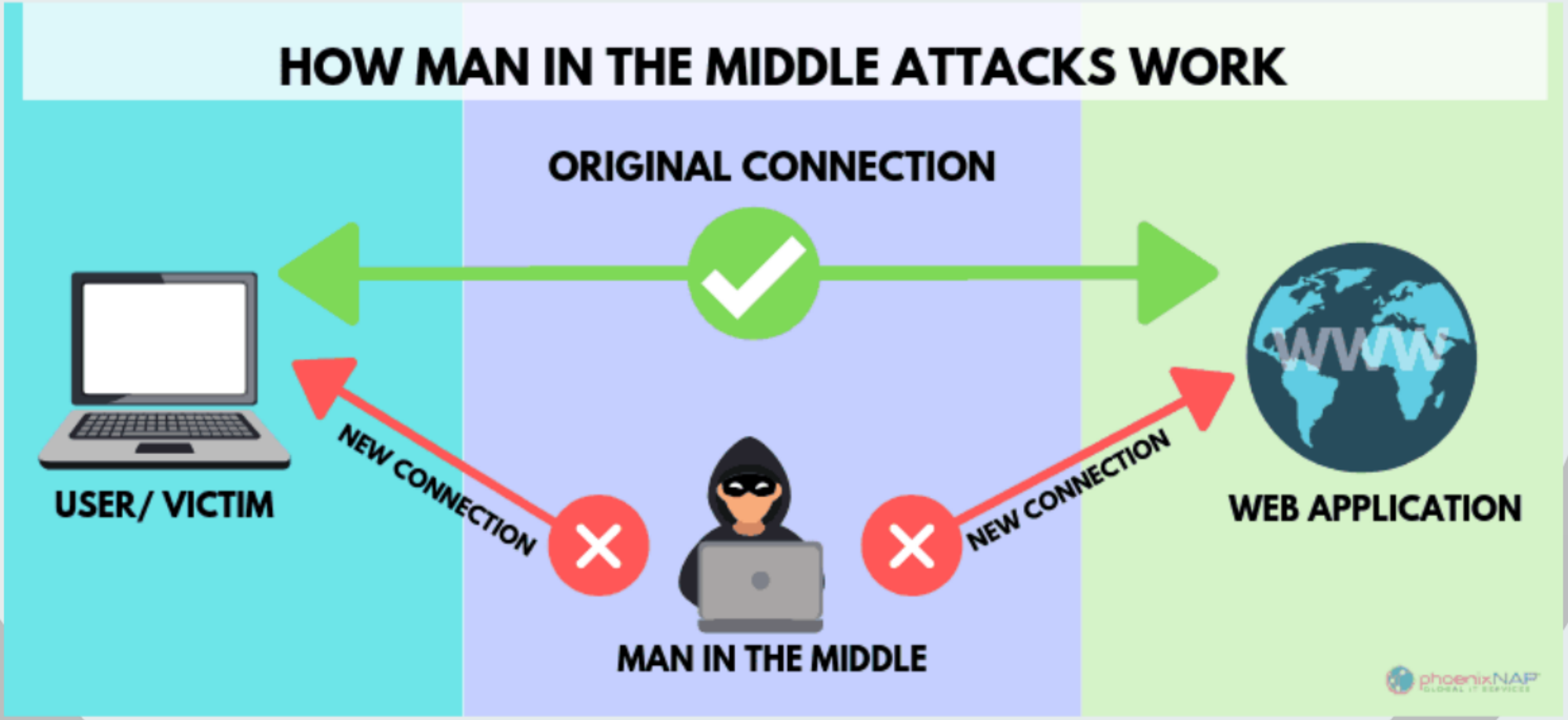


Bait & Switch

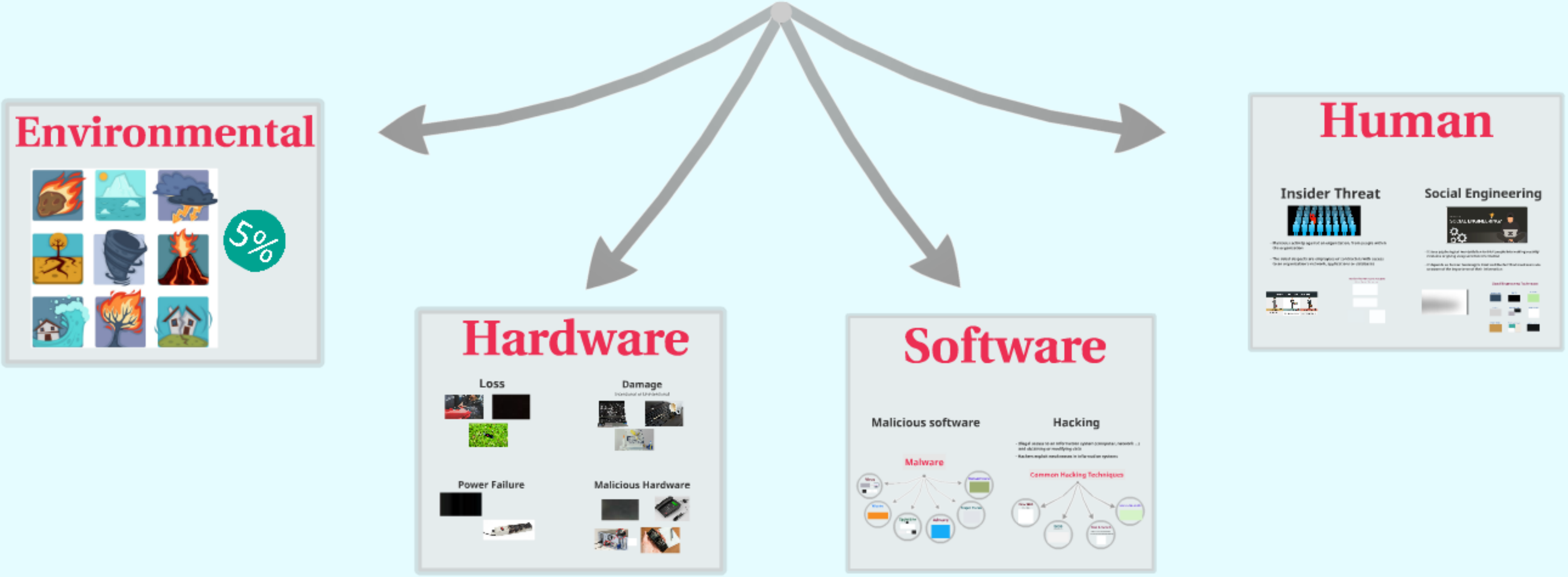
- The attacker can buy advertising spaces on the websites
- When a user clicks on the ad, he get directed to an infected page



Man-in-the-middle



Threat



Environmental

5%

Hardware

Loss

Damage

Intentional or Unintentional

Power Failure

Malicious Hardware

Software

Malicious software

Hacking

Malware

Common Hacking Techniques

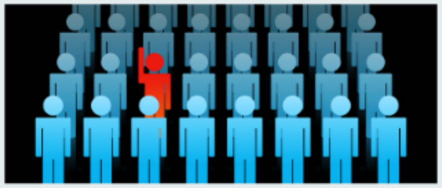
Human

Insider Threat

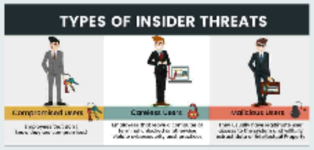
Social Engineering

Human

Insider Threat

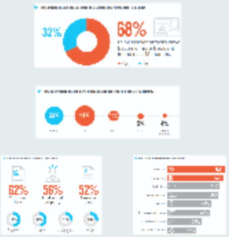


- Malicious activity against an organization, from people within the organization
- The usual suspects are employees or contractors with access to an organization's network, applications or databases

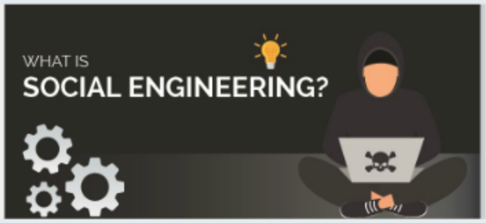


Insider threats report for 2019

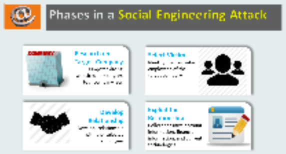
Source: cybersecurity-insiders.com



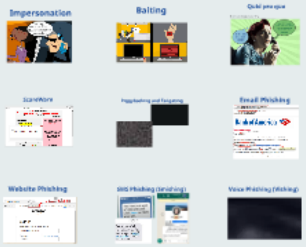
Social Engineering



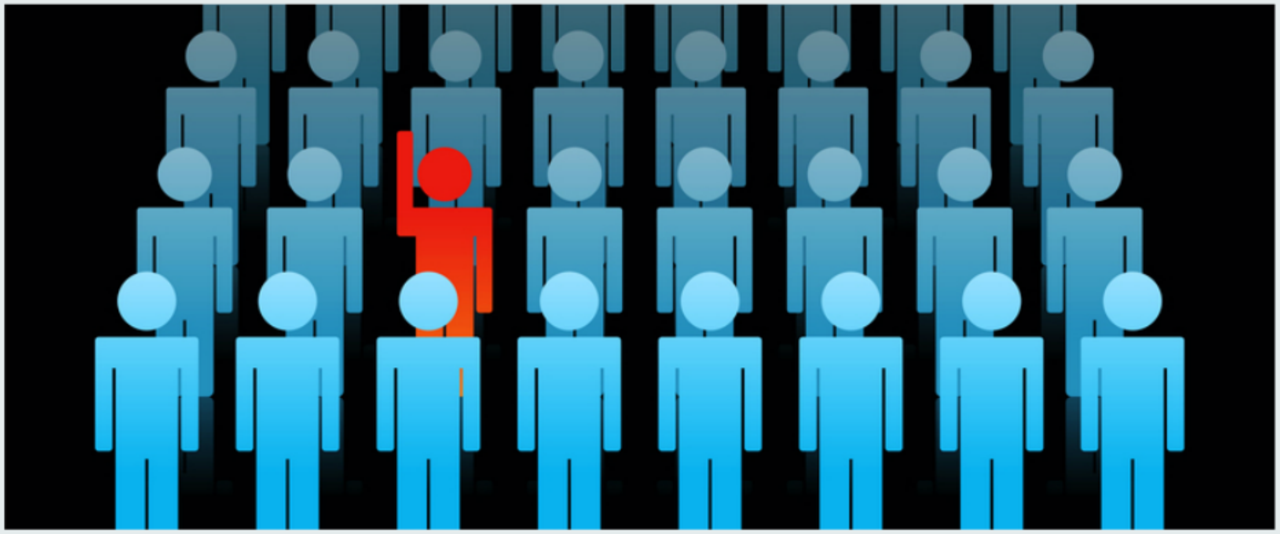
- It uses psychological manipulation to trick people into making security mistakes or giving away sensitive information
- It depends on human tendency to trust and the fact that most users are unaware of the importance of their information



Social Engineering Techniques

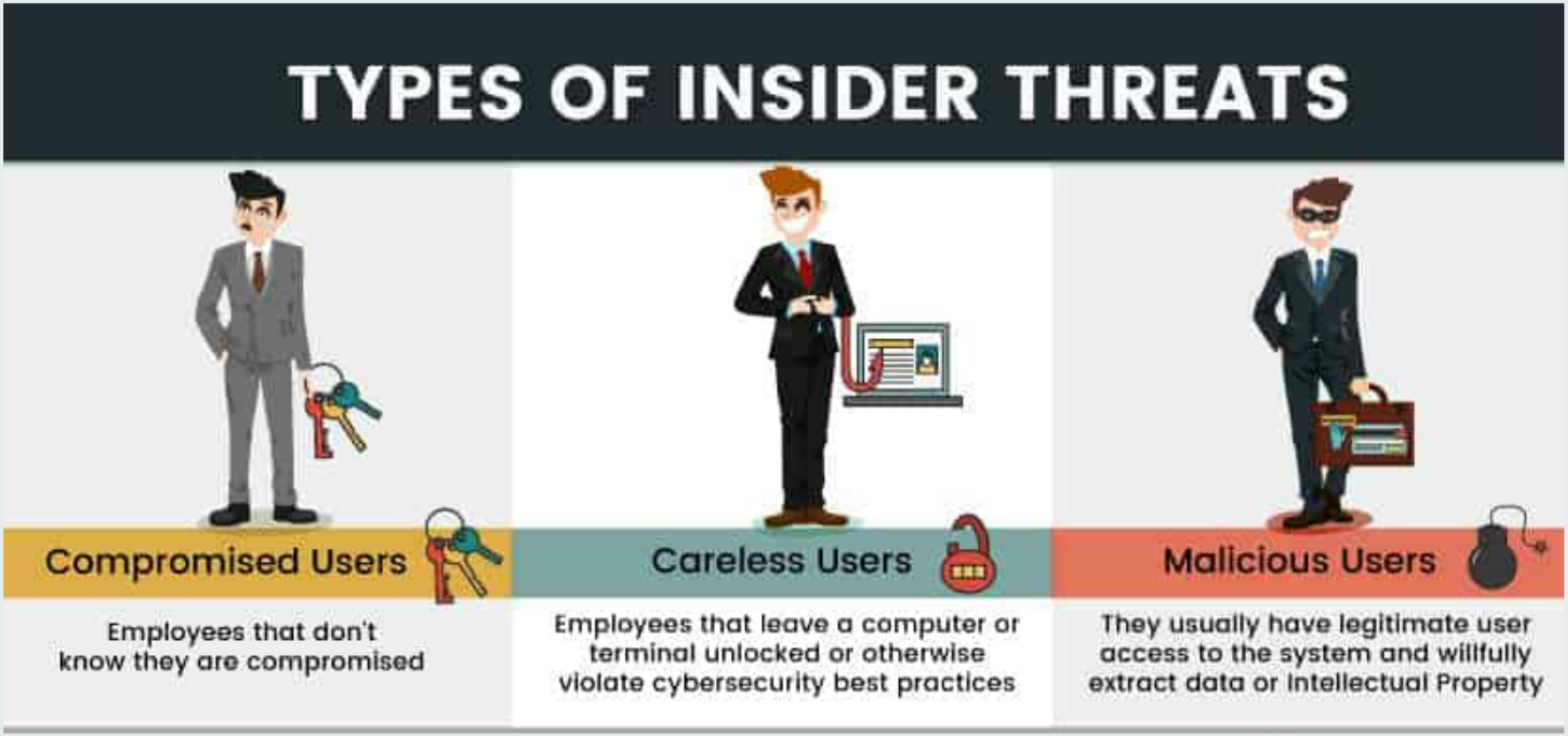


Insider Threat



- Malicious activity against an organization, from people within the organization

- The usual suspects are employees or contractors with access to an organization's network, applications or databases



TYPES OF INSIDER THREATS

Compromised Users

Employees that don't know they are compromised

Careless Users

Employees that leave a computer or terminal unlocked or otherwise violate cybersecurity best practices

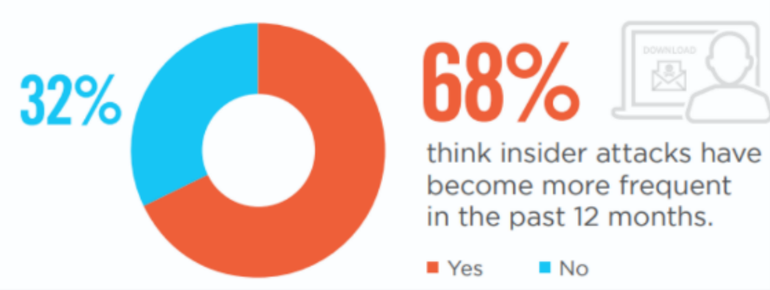
Malicious Users

They usually have legitimate user access to the system and willfully extract data or Intellectual Property

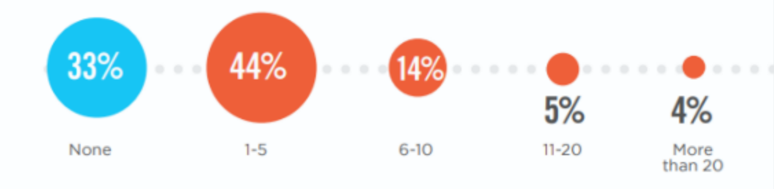
Insider threats report for 2019

Source: cybersecurity-insiders.com

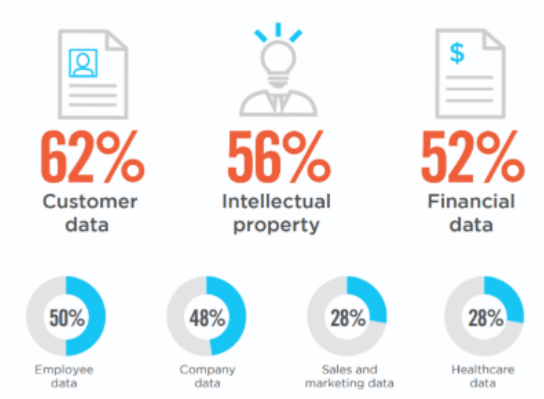
Have insider attacks become more or less frequent over the last 12 months?



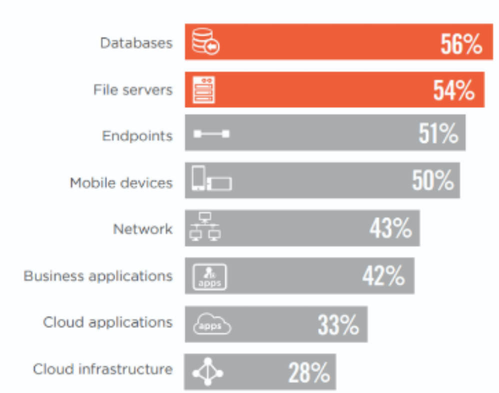
How many insider attacks did your organization experience in the last 12 months?



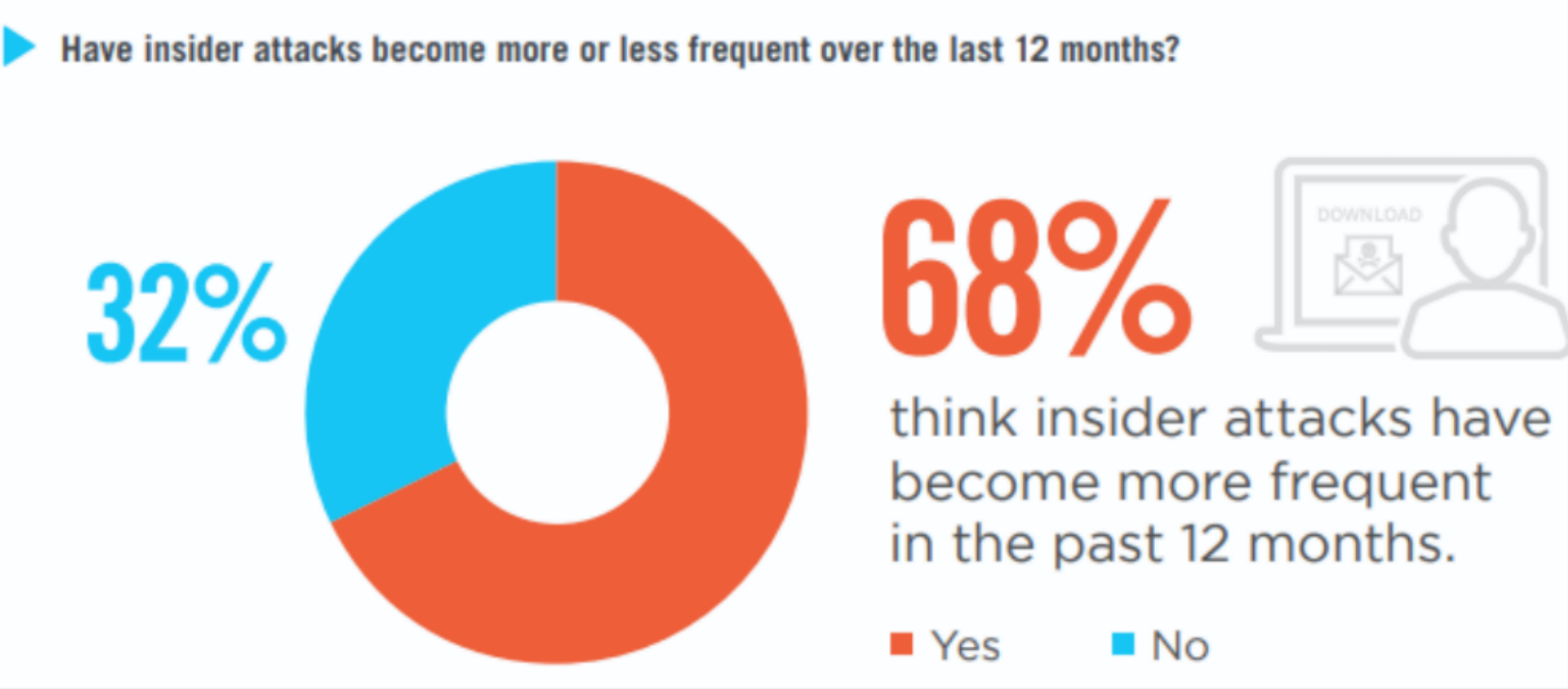
What types of data are most vulnerable to insider attacks?



What IT assets are most vulnerable to insider attacks?



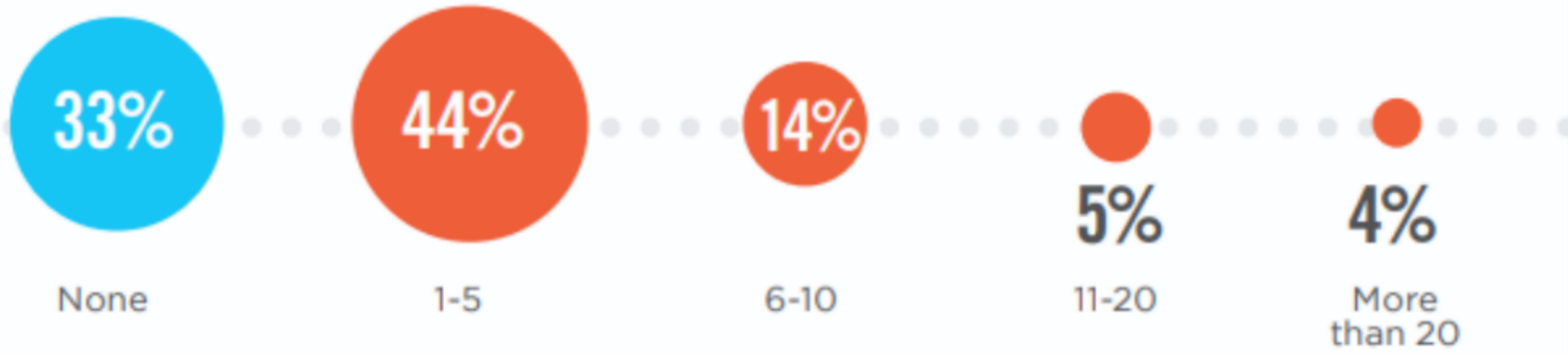
Source: cybersecurity-insiders.com



Have insider attacks become more or less frequent over the last 12 months?

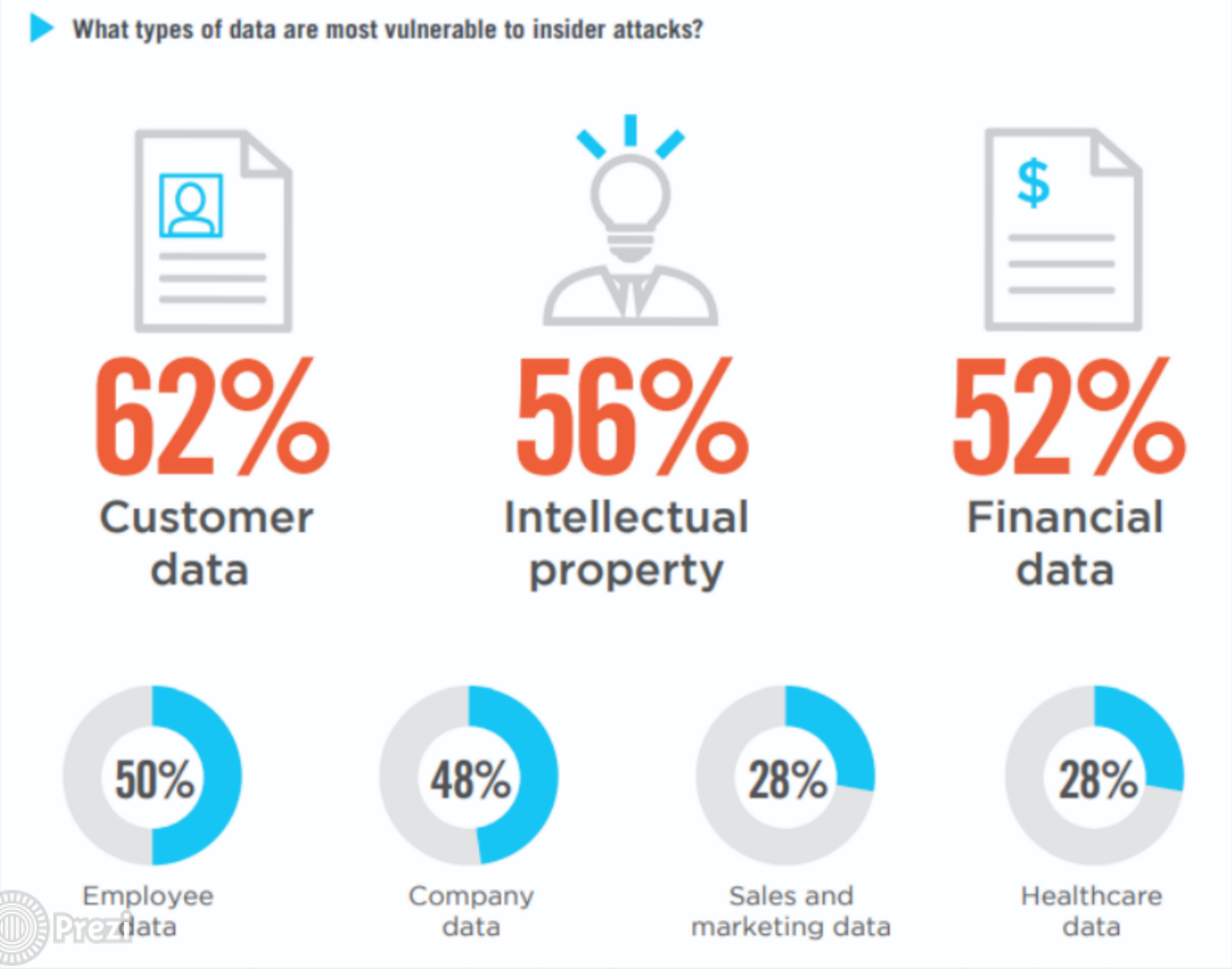
68% think insider attacks have become more frequent in the past 12 months.

How many insider attacks did your organization experience in the last 12 months?



nerable to insider attacks?

What IT assets are most vulnerable to insider at



What types of data are most vulnerable to insider attacks?

62% Customer data

56% Intellectual property

52% Financial data

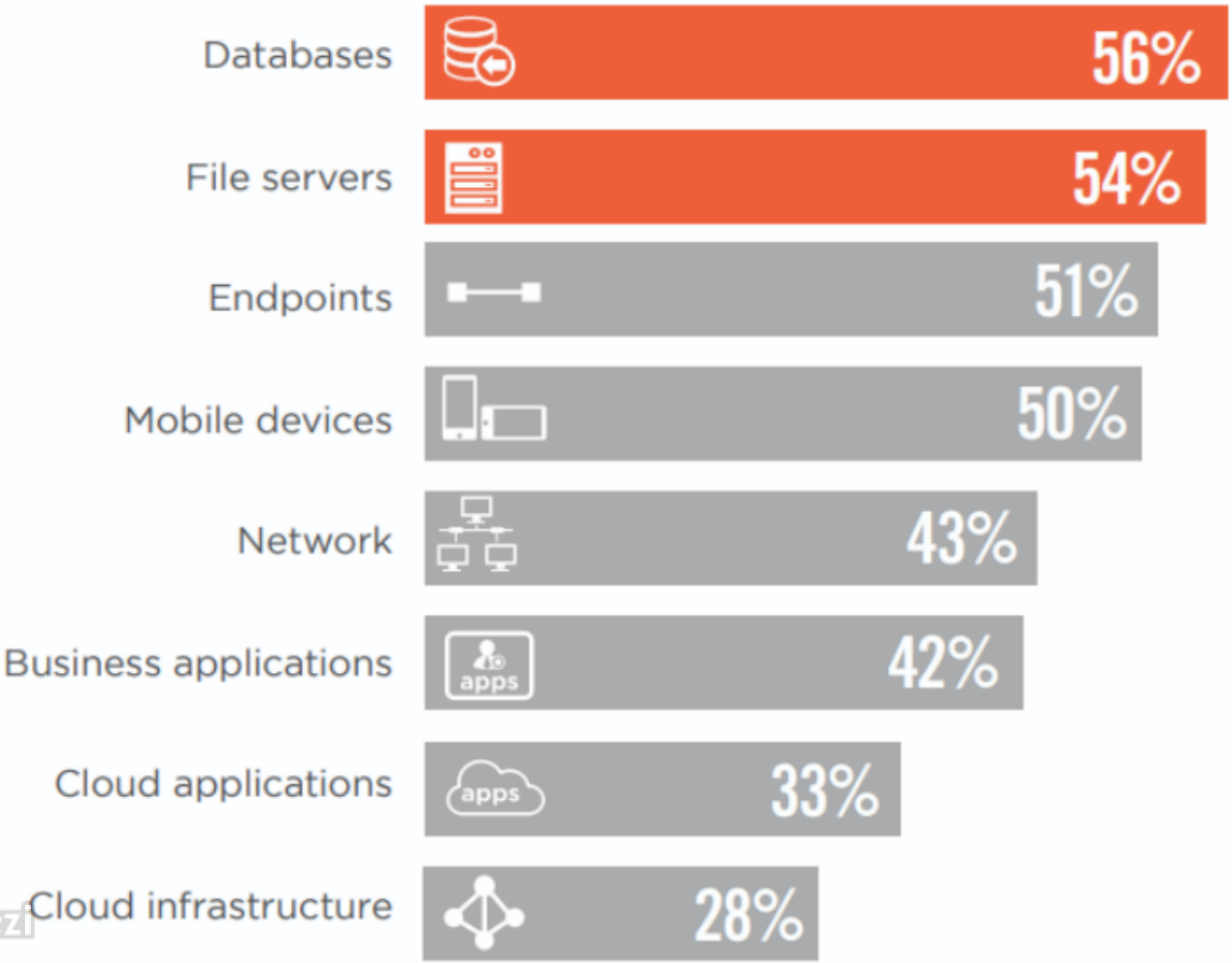
50% Employee data

48% Company data

28% Sales and marketing data

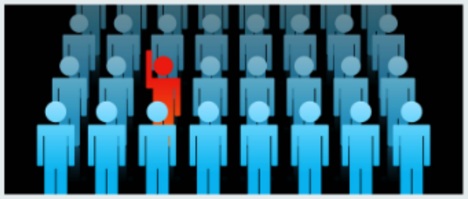
28% Healthcare data

What IT assets are most vulnerable to insider attacks?

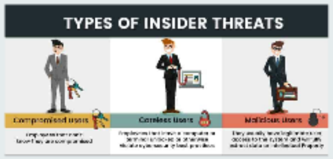


Human

Insider Threat

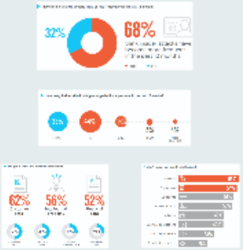


- Malicious activity against an organization, from people within the organization
- The usual suspects are employees or contractors with access to an organization's network, applications or databases

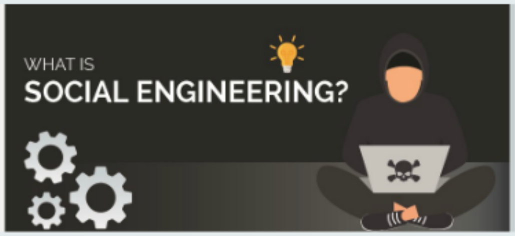


Insider threats report for 2019

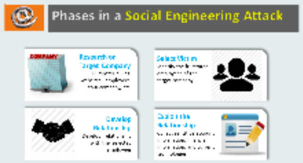
Source: cybersecurity-insiders.com



Social Engineering



- It uses psychological manipulation to trick people into making security mistakes or giving away sensitive information
- It depends on human tendency to trust and the fact that most users are unaware of the importance of their information



Social Engineering Techniques

Impersonation

Baiting

Quid pro quo

ScareWare

Piggybacking and tailgating

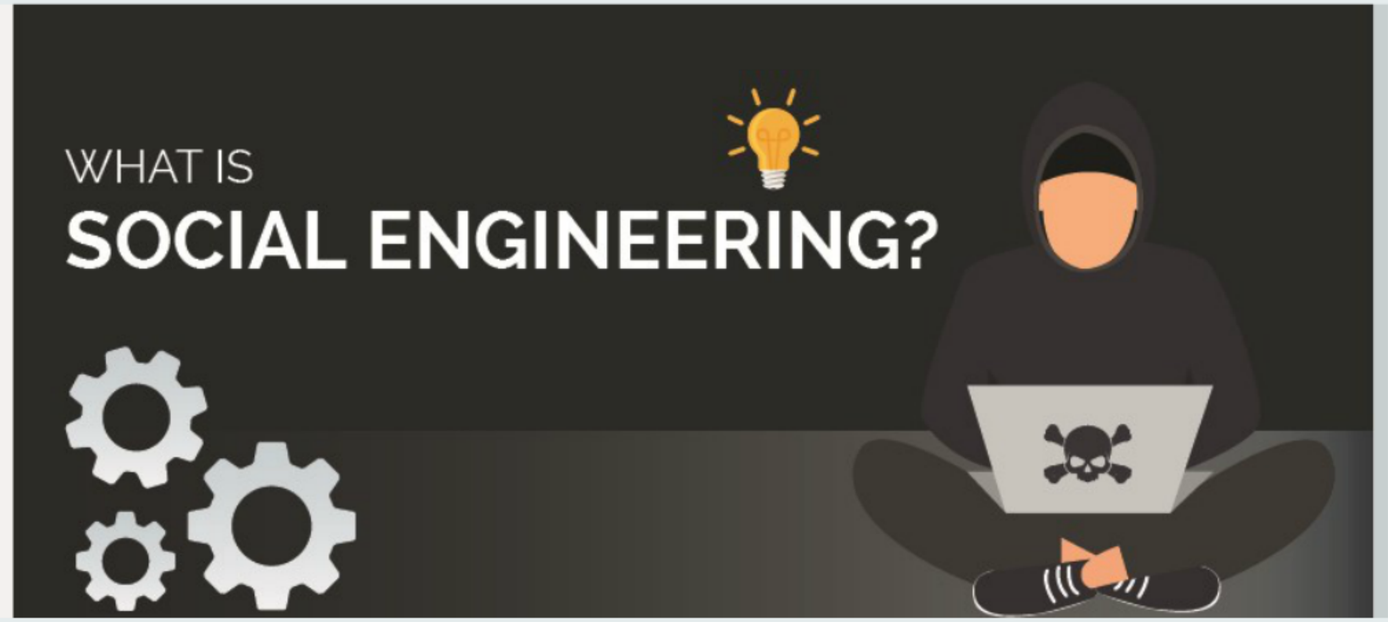
Email Phishing

Website Phishing

SMS Phishing (Smishing)

Voice Phishing (Vishing)

Social Engineering



- It uses psychological manipulation to trick people into making security mistakes or giving away sensitive information

- It depends on human tendency to trust and the fact that most users are unaware of the importance of their information

Phases in a Social Engineering Attack

Research on Target Company

Dumpster diving, websites, employees, tour company, etc.

Select Victim

Identify the frustrated employees of the target company

Develop Relationship

Develop relationship with the selected employees

Exploit the Relationship

Collect sensitive account information, financial information, and current technologies

Social Engineering Techniques

Impersonation

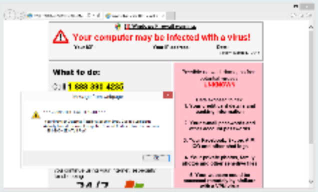
Baiting

Quid pro quo

Means something for something:

OH MY! I THINK IT'S A SOCIAL ENGINEER!
Now if I could just get your User ID and password I can fix the problem.

ScareWare



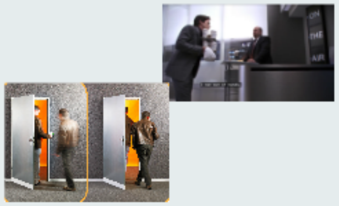
Your computer may be infected with a virus!

What to do:

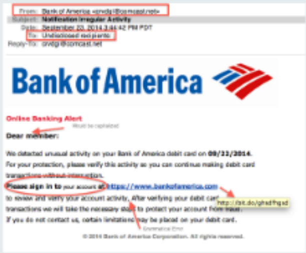
Call 1 888 398 4285

24/7

Piggybacking and Tailgating



Email Phishing



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 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.

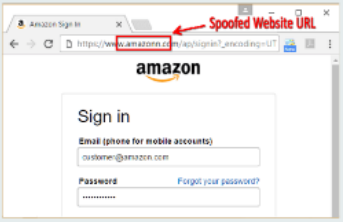
If you do not contact us, certain limitations may be placed on your debit card.

http://bit.do/ghsdfhgsd

Grammatical Error

© 2014 Bank of America Corporation. All rights reserved.

Website Phishing



Sign in

Email (phone for mobile accounts)

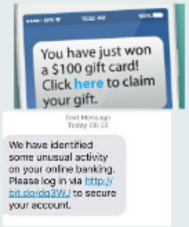
customer@amazon.com

Password

Forgot your password?

••••••••••••

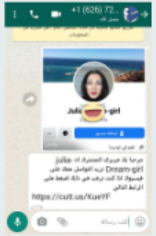
SMS Phishing (Smishing)



You have just won a $100 gift card! Click here to claim your gift.

Text Message
Today 08:53

We have identified some unusual activity on your online banking. Please log in via http://bit.do/dq3WJ to secure your account.



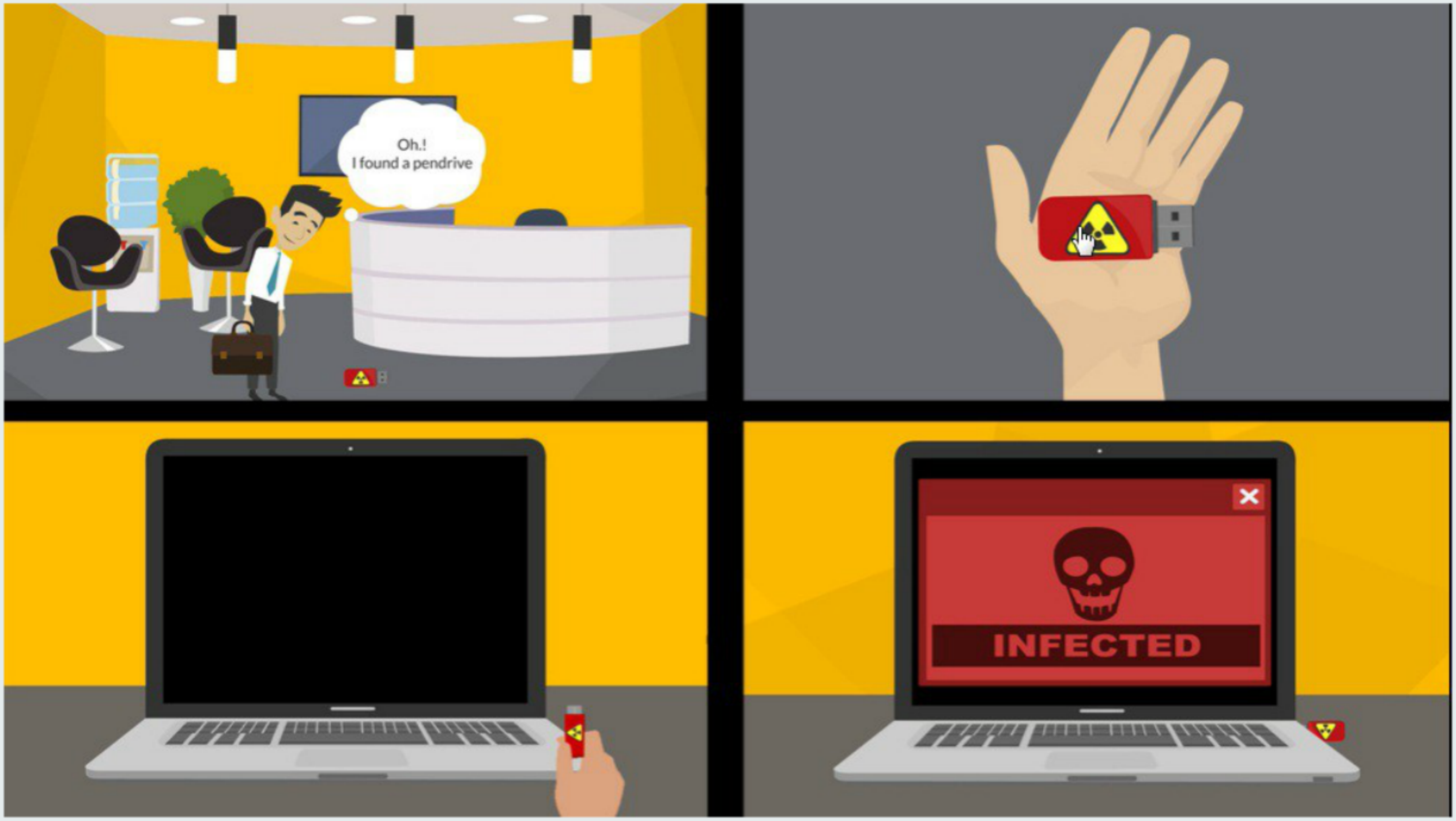
https://cutt.us/KueYF

Voice Phishing (Vishing)

Impersonation

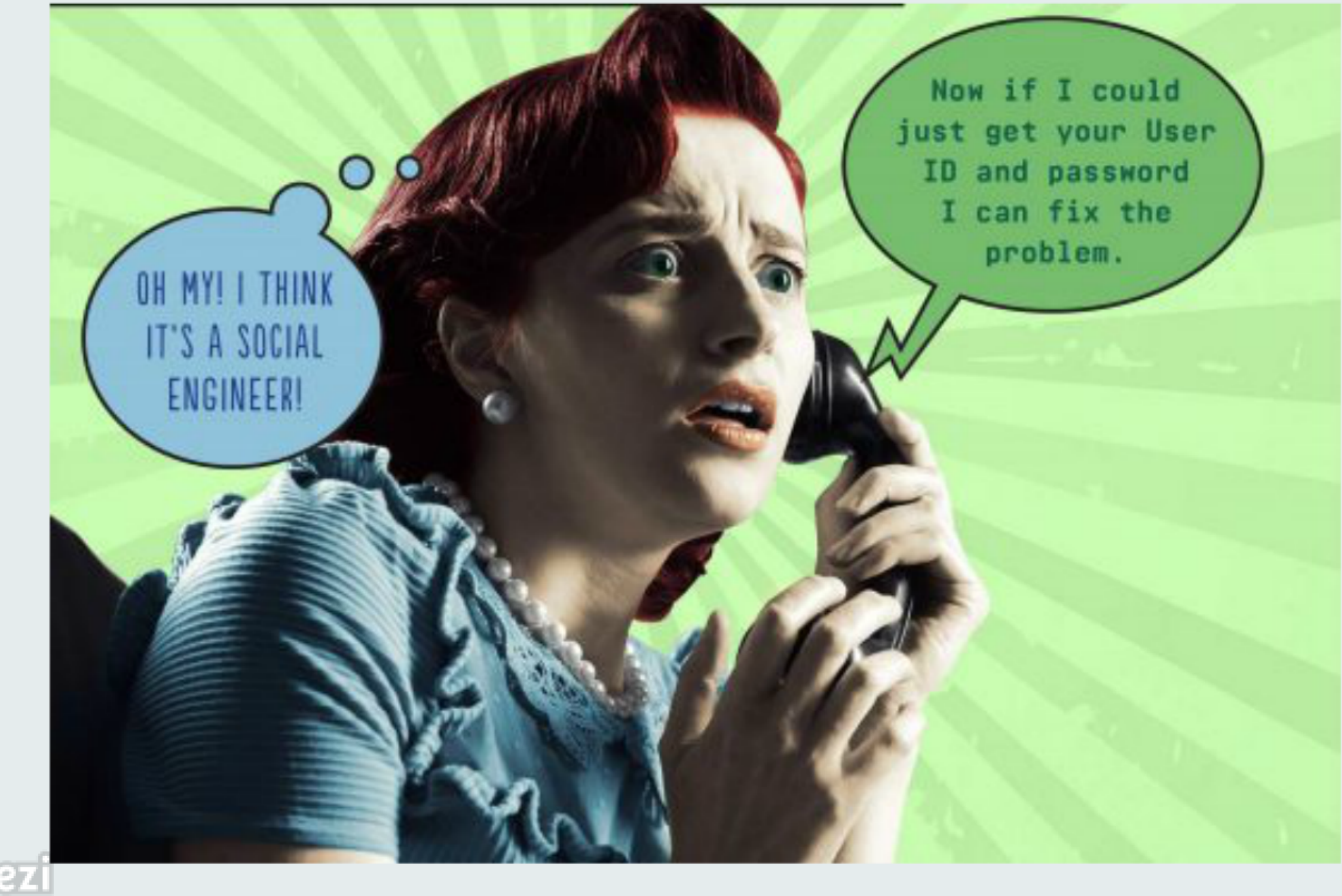
Hi Amy,
This is Joe, from IT...I'm working from home today...

Baiting

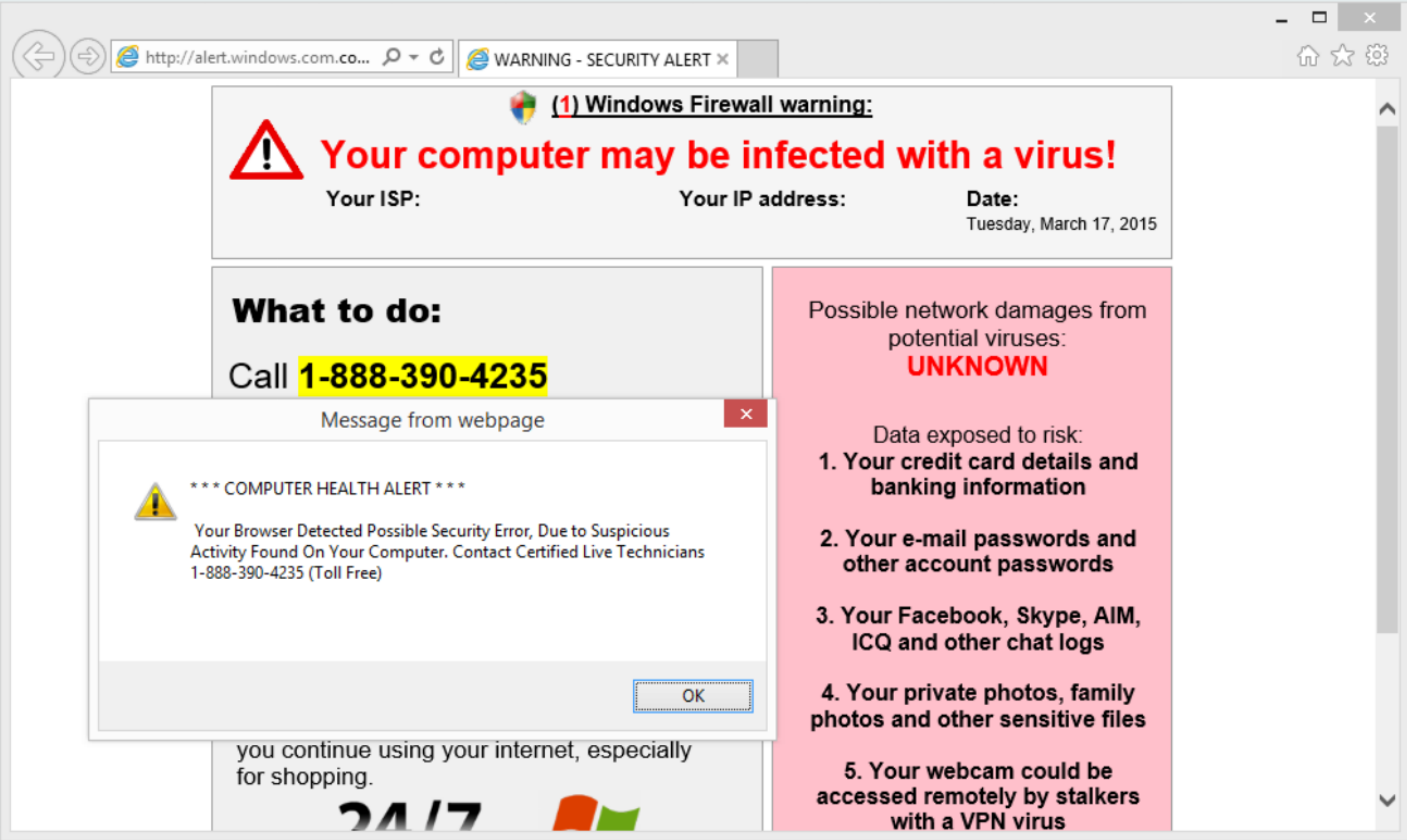


Quid pro quo

Means something for something:


OH MY! I THINK IT'S A SOCIAL ENGINEER!
Now if I could just get your User ID and password I can fix the problem.

ScareWare



(1) Windows Firewall warning:

Your computer may be infected with a virus!

Your ISP: **Your IP address:** **Date:** Tuesday, March 17, 2015

What to do:

Call **1-888-390-4235**

Message from webpage

* * * COMPUTER HEALTH ALERT * * *

Your Browser Detected Possible Security Error, Due to Suspicious Activity Found On Your Computer. Contact Certified Live Technicians 1-888-390-4235 (Toll Free)

you continue using your internet, especially for shopping.

24/7

Possible network damages from potential viruses:
UNKNOWN

Data exposed to risk:

1. Your credit card details and banking information

2. Your e-mail passwords and other account passwords

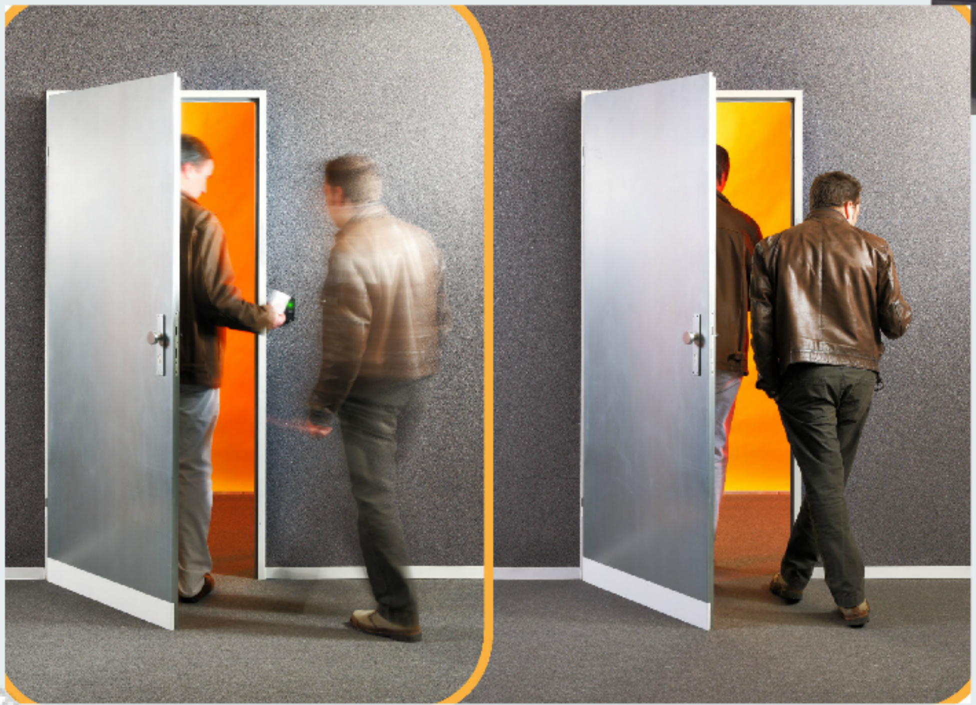
3. Your Facebook, Skype, AIM, ICQ and other chat logs

4. Your private photos, family photos and other sensitive files

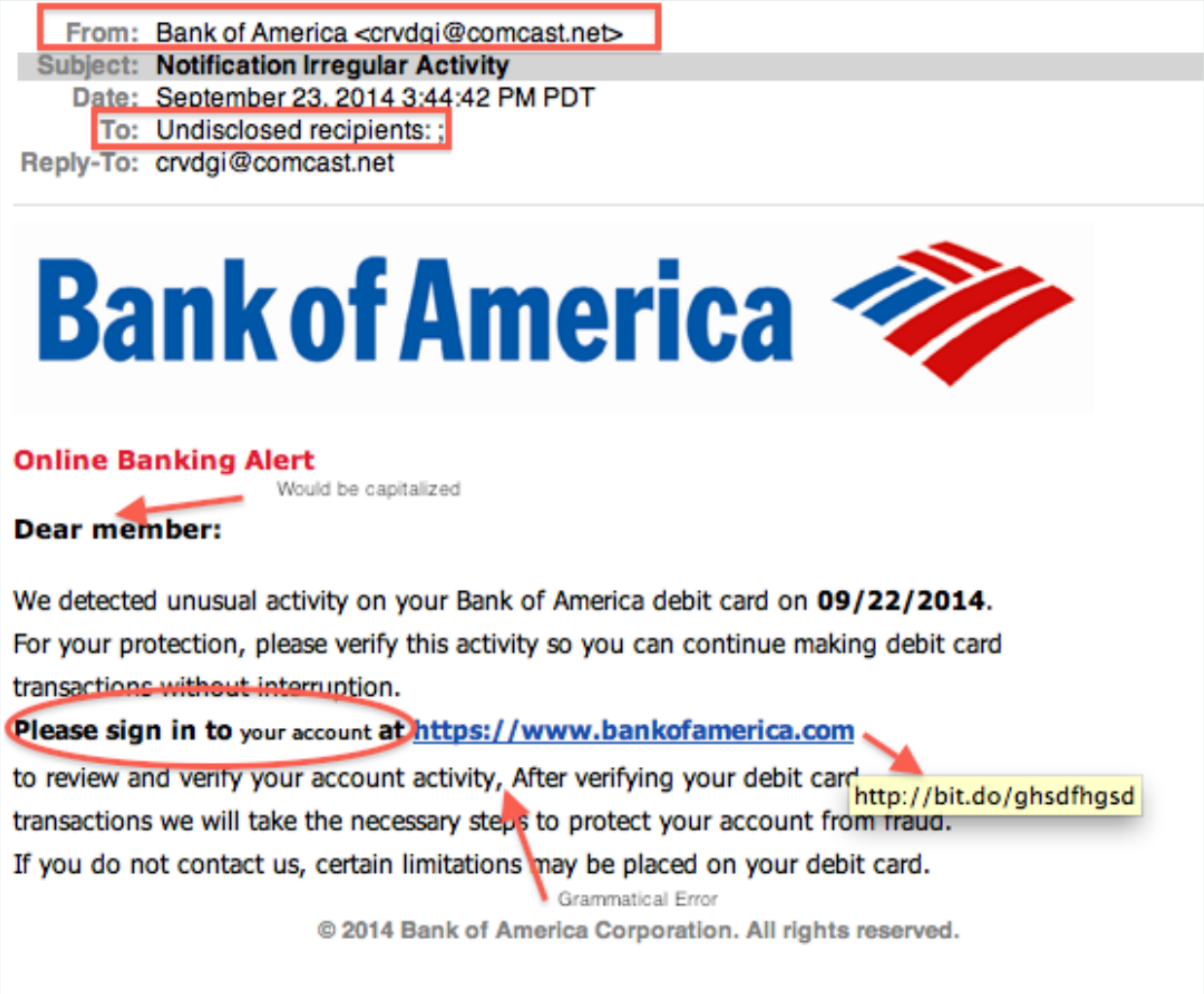
5. Your webcam could be accessed remotely by stalkers with a VPN virus

Prezi

Piggybacking and Tailgating



Email Phishing



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.

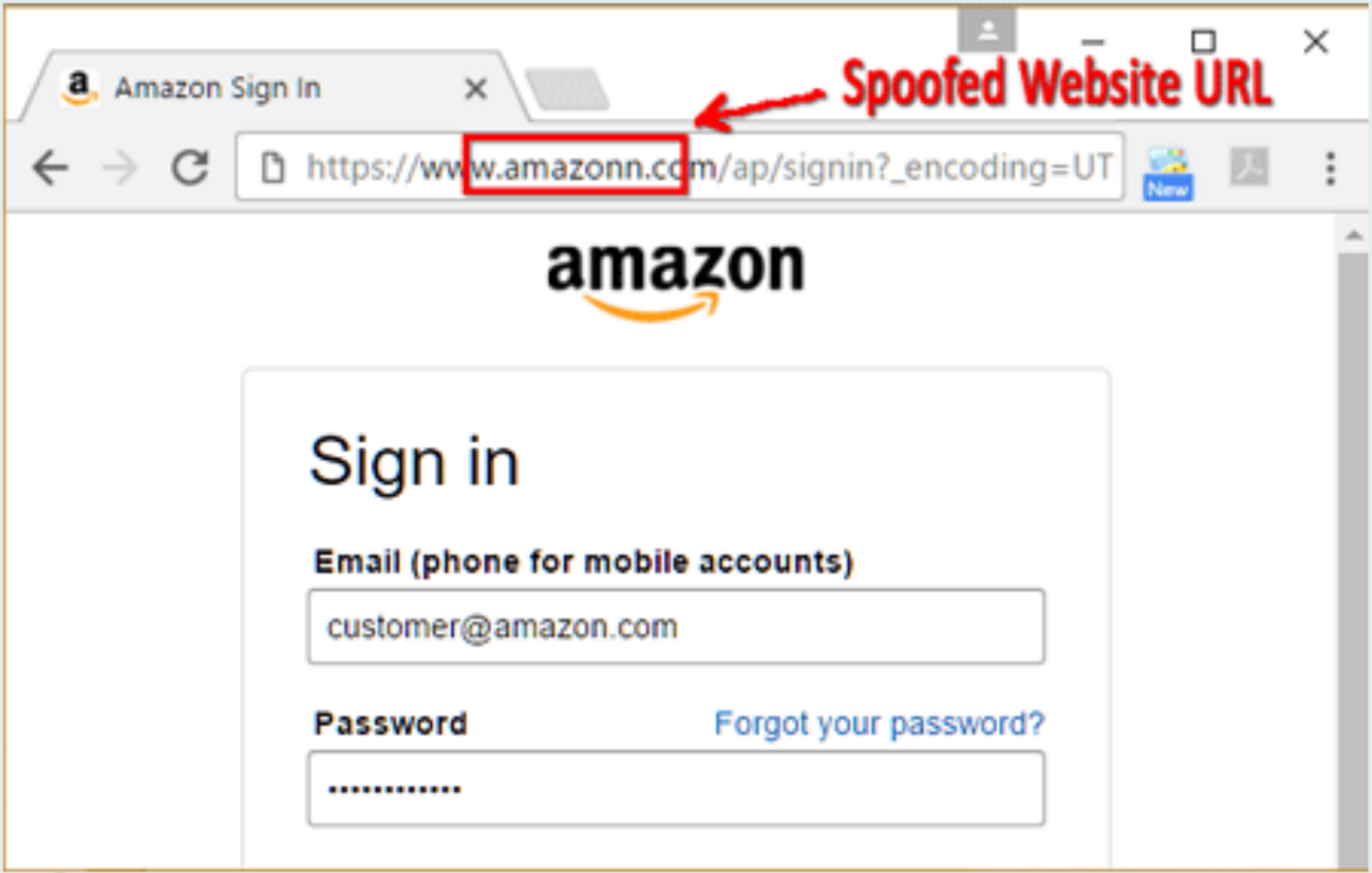
Please sign in to your account **at** https://www.bankofamerica.com to review and verify your account activity, After verifying your debit card transactions we will take the necessary steps to protect your account from fraud. If you do not contact us, certain limitations may be placed on your debit card.

http://bit.do/ghsdfhgsd

Grammatical Error

© 2014 Bank of America Corporation. All rights reserved.

Website Phishing



Spoofed Website URL

https://www.amazonn.com/ap/signin?_encoding=UT

Sign in

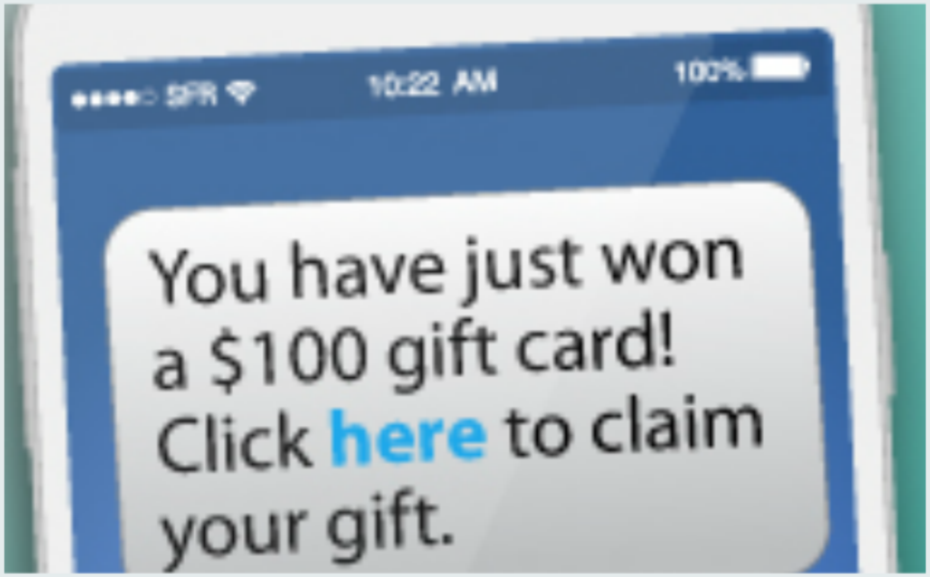
Email (phone for mobile accounts)

customer@amazon.com

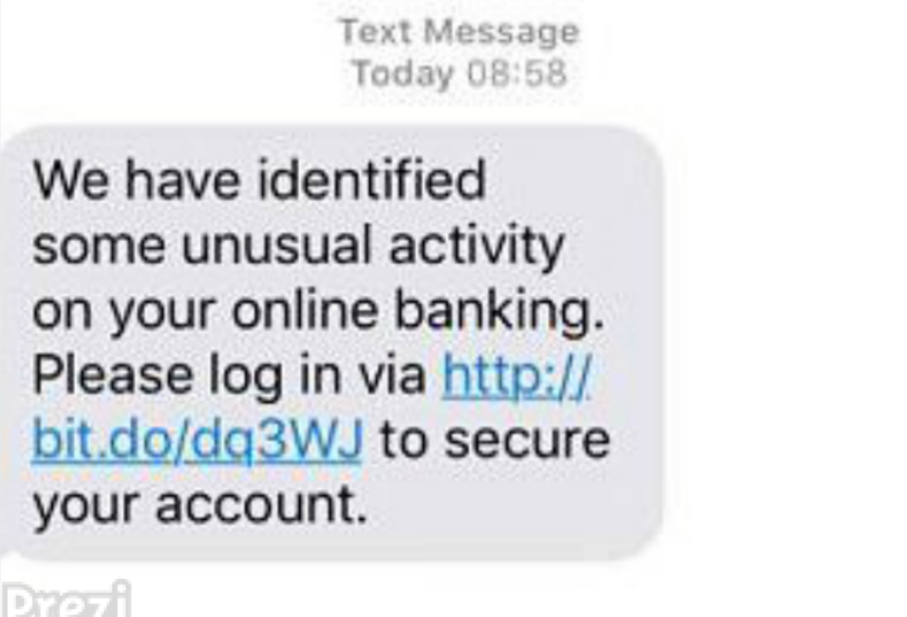
Password

•••••••••••••

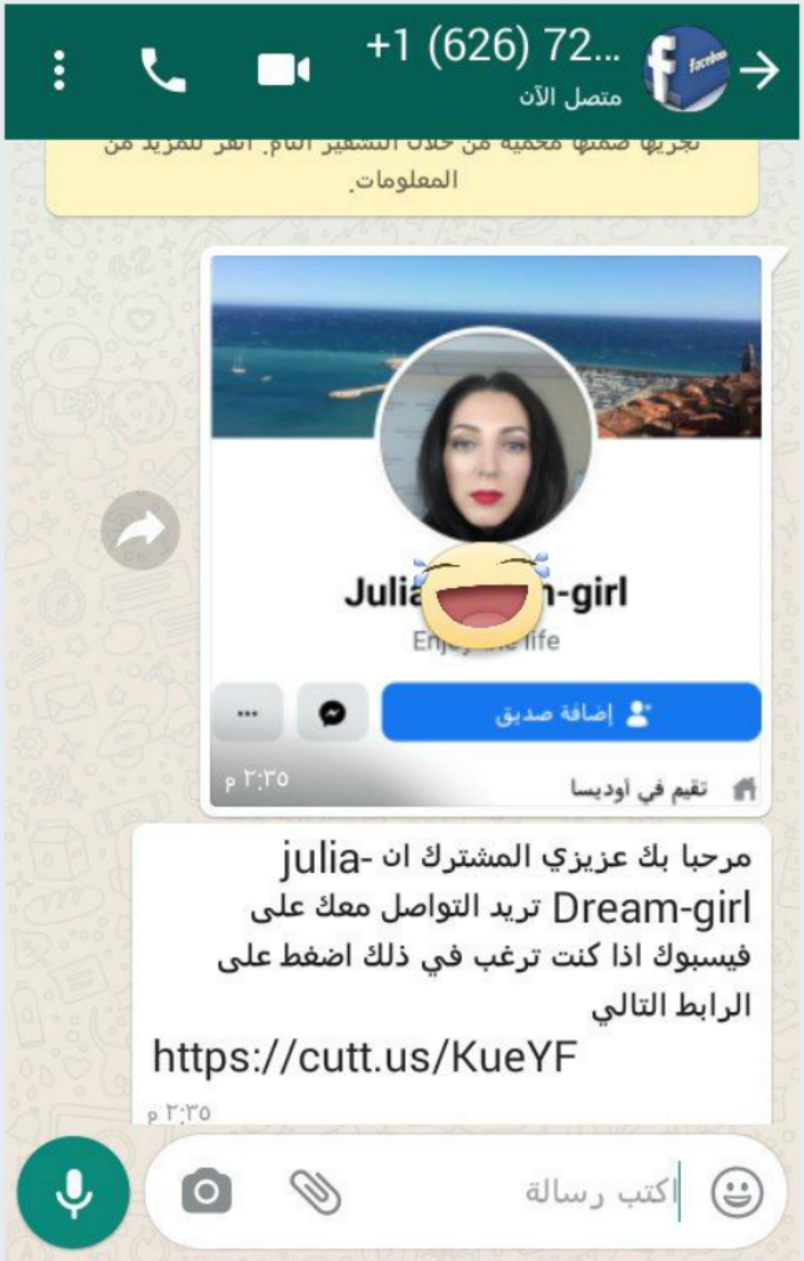
SMS Phishing (Smishing)



You have just won a $100 gift card! Click here to claim your gift.



We have identified some unusual activity on your online banking. Please log in via http://bit.do/dq3WJ to secure your account.



تجريها ضمنها محمية من خلال التشفير التام. انقر للمزيد من
المعلومات.

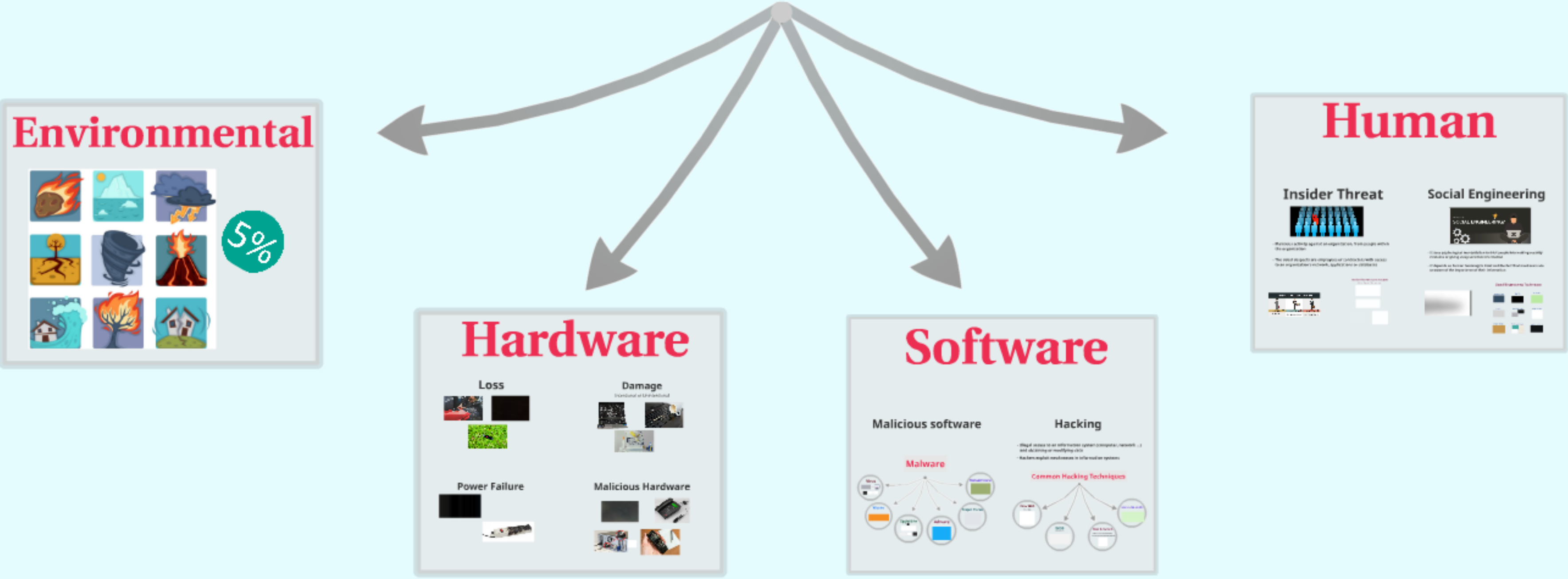
مرحبا بك عزيزي المشترك ان julia-
Dream-girl تريد التواصل معك على
فيسبوك اذا كنت ترغب في ذلك اضغط على
الرابط التالي
https://cutt.us/KueYF

٢:٣٥ م

Voice Phishing (Vishing)

Voice Phishing (Vishing)

Threat



Environmental

5%

Hardware

Loss

Damage

Power Failure

Malicious Hardware

Software

Malicious software

Hacking

Malware

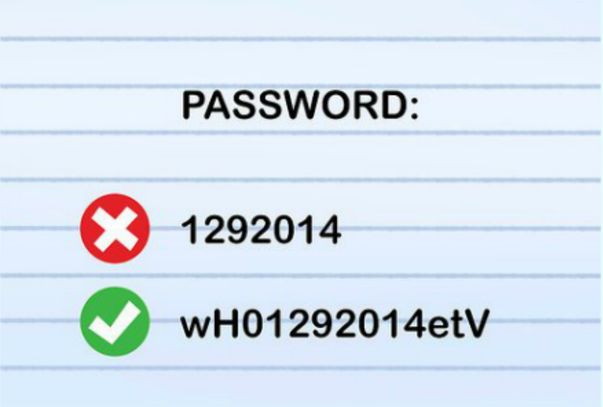
Common Hacking Techniques

Human

Insider Threat

Social Engineering

AppStore Play Store Microsoft Store



PASSWORD:

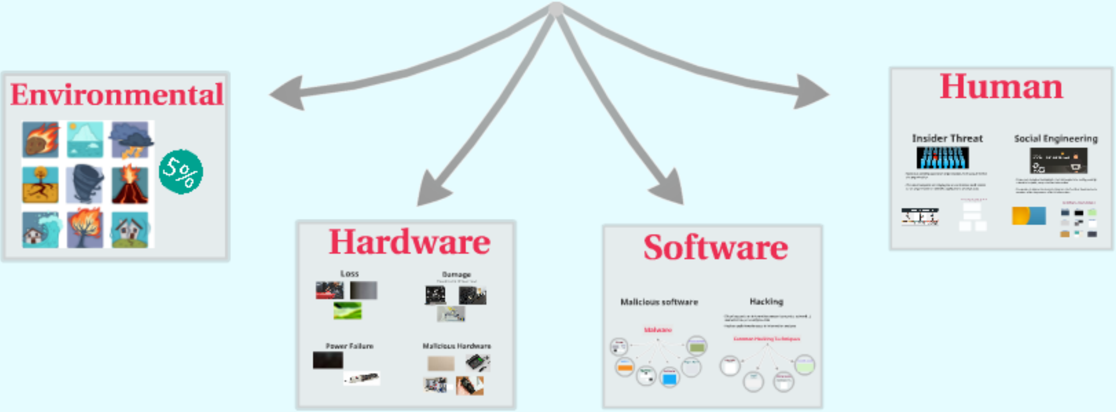
✗ 1292014

✓ wH01292014etV

Security Tip

Be careful when opening attachments sent via email.

Threat



Environmental

Hardware

Loss

Damage

Power Failure

Malicious Hardware

Software

Malicious software

Hacking

Malware

Common Hacking Techniques

Human

Insider Threat

Social Engineering

Countermeasures

People

- Training and Awareness.
- Physical Security.
- Emergency Drills.
- ...

Technology

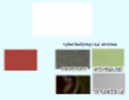
- SIEM solution.
  Security Information & Event Management.
- DLP solution.
  Data Leakage Prevention.
- IAM solution.
  Identity and Access Management.
- Encryption.
- Firewall, Anti-spam, Anti-Malware...

Process

ISO/IEC 27001

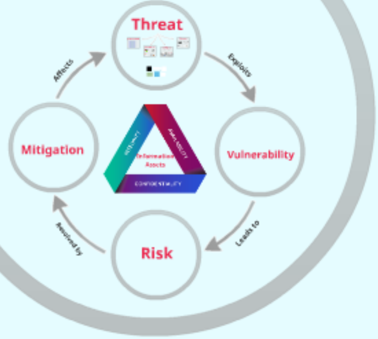
CyberCrime

Cyber-Bullying



Cyber-Extortion

Information Security



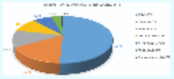
Agenda

- Preface
- Information Security
- CyberSecurity Threats
- Countermeasures
- CyberCrime

Thank You

APPS
Information Communication Technology

Preface



Countermeasures

People

- Training and Awareness.
- Physical Security.
- Emergency Drills.
- ....

Technology

- SIEM solution.
  Security Information & Events Management.
- DLP solution.
  Data Leakage Prevention.
- IAM solution.
  Identity and Access Management.
- Encryption.
- Firewall, Anti-spam, Anti-Malware...

Process

Processes are important so that people can optimally operate and manage technologies to ensure **information security** and **business continuity**.

ISO/IEC 27001

It's the **international standard** that helps organizations manage their information security by addressing people and processes as well as technology.

It details requirements for establishing, implementing, maintaining an **information security management system (ISMS).**

What is ISMS?

[illegible]

People

- Training and Awareness.
- Physical Security.
- Emergency Drills.
- ....

T

- SIEM s
  Security In
- DLP so
  Data Leaka
- IAM so
  Identity an
- Encryp
- Firewa

Process

ess.

Technology

- SIEM solution.
  Security Information & Events Management.
- DLP solution.
  Data Leakage Prevention.
- IAM solution.
  Identity and Access Management.
- Encryption.
- Firewall, Anti-spam, Anti-Malware…

Process

Process

Processes are important so that people can optimally operate and manage technologies to ensure **information security** and **business continuity**.

ISO/IEC 27001

It's the **international standard** that helps organizations manage their information security by addressing people and processes as well as technology.

It details requirements for establishing, implementing, maintaining an **information security management system (ISMS).**

What is ISMS?

An ISMS is a holistic approach to securing the confidentiality, integrity and availability (CIA) of corporate information assets.

It consists of policies, procedures and other controls involving people, processes and technology.

Policy examples:

- Back-up
- Information classification
- Communication Security
- Mobile device and teleworking
- Protection from malware
- Password policy

ISO/IEC 27001

It's the **international standard** that helps organizations manage their information security by addressing people and processes as well as technology.

It details requirements for establishing, implementing, maintaining an **information security management system (ISMS).**

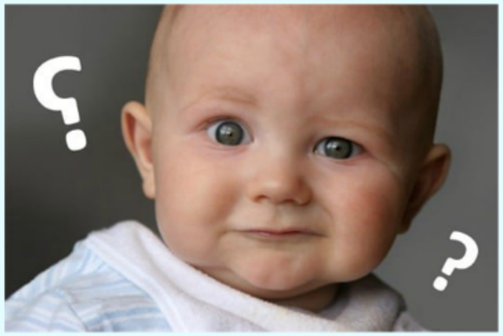
What is ISMS?

An ISMS is a holistic approach to securing the confidentiality, integrity and availability (CIA) of corporate information assets.

It consists of policies, procedures and other controls involving people, processes and technology.

Policy examples:

- Back-up
- Information classification
- Communication Security
- Mobile device and teleworking
- Protection from malware
- Password policy



What is ISMS?

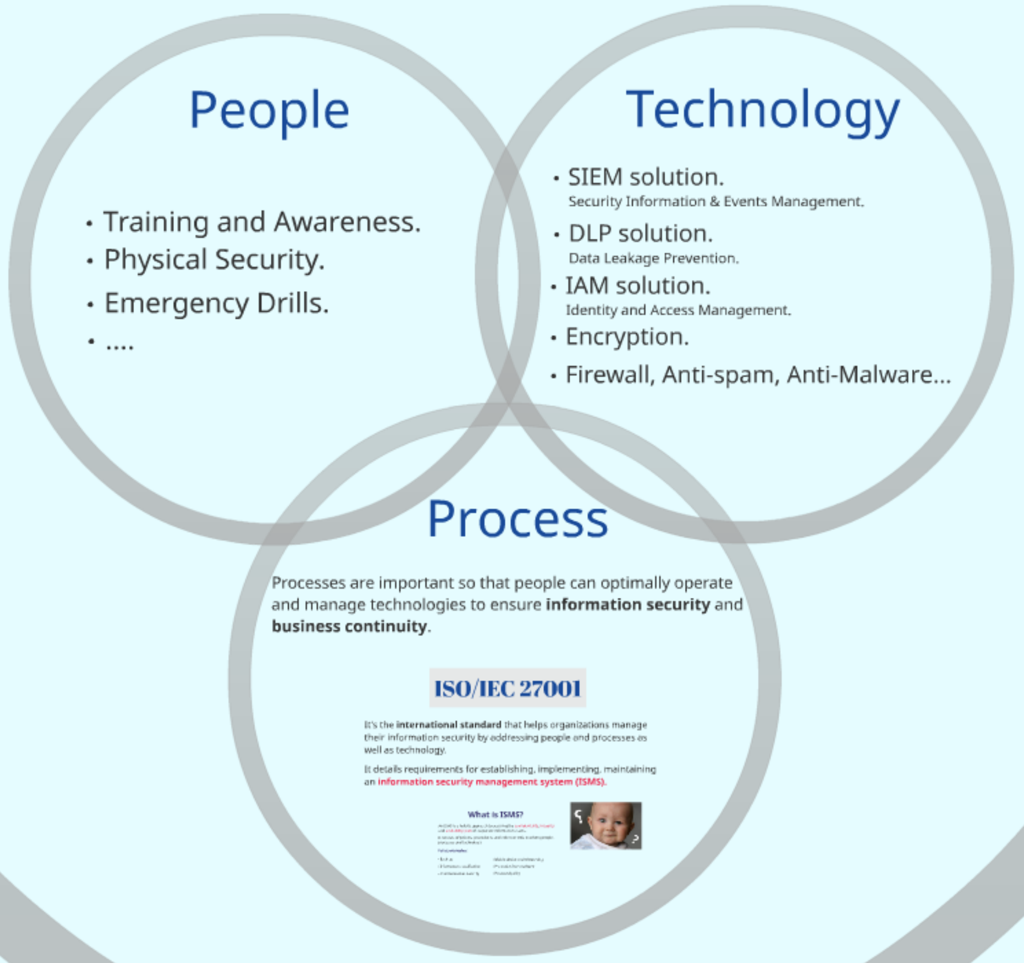
An ISMS is a holistic approach to securing the confidentiality, integrity and availability (CIA) of corporate information assets.

It consists of policies, procedures and other controls involving people, processes and technology.

Policy examples:

- Back-up
- Information classification
- Communication Security
- Mobile device and teleworking
- Protection from malware
- Password policy

Countermeasures



People

- Training and Awareness.
- Physical Security.
- Emergency Drills.
- ....

Technology

- SIEM solution.
  Security Information & Events Management.
- DLP solution.
  Data Leakage Prevention.
- IAM solution.
  Identity and Access Management.
- Encryption.
- Firewall, Anti-spam, Anti-Malware...

Process

Processes are important so that people can optimally operate and manage technologies to ensure **information security** and **business continuity**.

ISO/IEC 27001

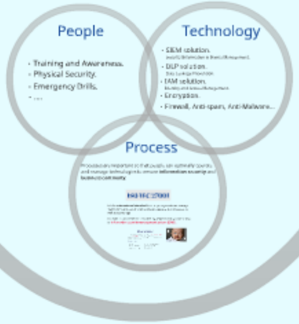
It's the **international standard** that helps organizations manage their information security by addressing people and processes as well as technology.

It details requirements for establishing, implementing, maintaining an **information security management system (ISMS).**

What is ISMS?

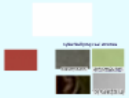
[illegible]

Countermeasures



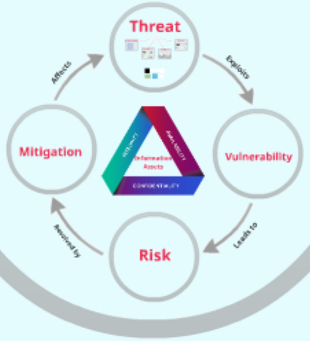
CyberCrime

Cyber-Bullying



Cyber-Extortion

Information Security



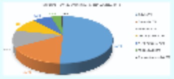
Agenda

- Preface
- Information Security
- CyberSecurity Threats
- Countermeasures
- CyberCrime

Thank You

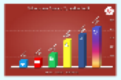
APPS
Information Communication Technology

Preface



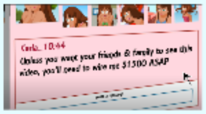
CyberCrime

Cyber-Bullying

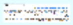


Cyberbullying real stories

Cyber-Extortion



Carla 10:44
Unless you want your friends & family to see this video, you'll need to wire me $1500 ASAP

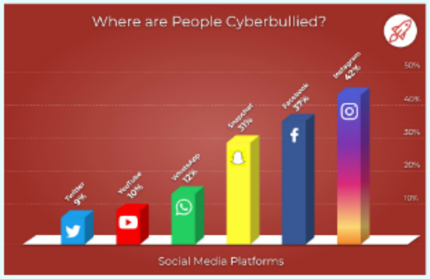


[illegible]

What to do?

[illegible]

Cyber-Bullying

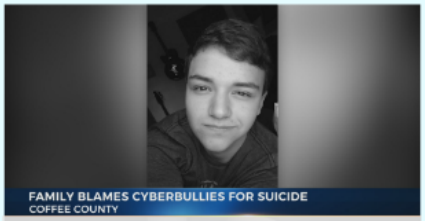


Cyberbullying real strories

Barndy Vela's sister said that people made fake dating profiles of her sister.

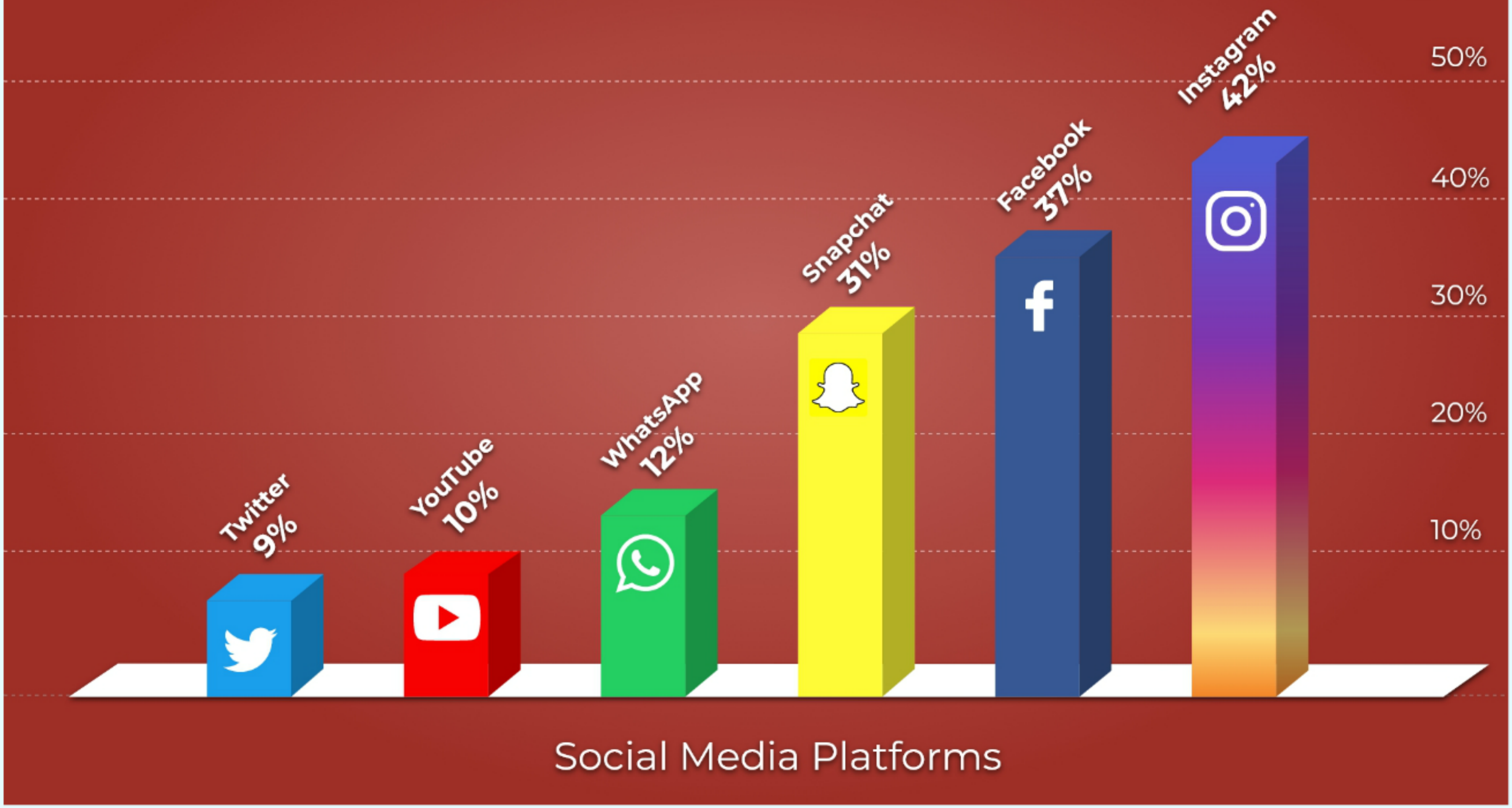
NEWS ROOM
GIRLS SUSPECTED OF CYBER-BULLYING TEEN
Police: Rebecca Sedwick killed herself after being bullied
LIVE
CNN

Screenshots of "anonymous" comments made to Rebecca on Ask.fm, saying things like "Nobody cares about you" and "you seriously deserve to die."

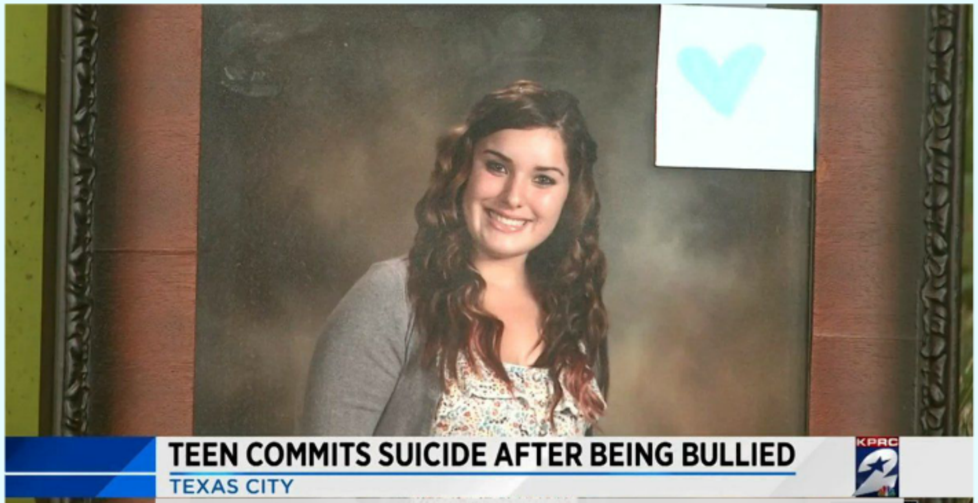


Channing Smith' family says his classmates posted a screenshot on Instagram and Snapchat of text messages between Channing and another boy.

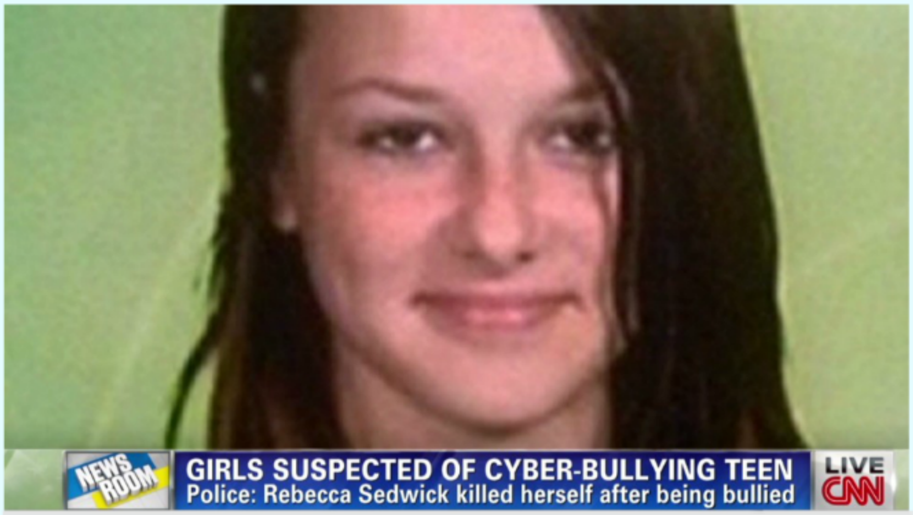
Where are People Cyberbullied?



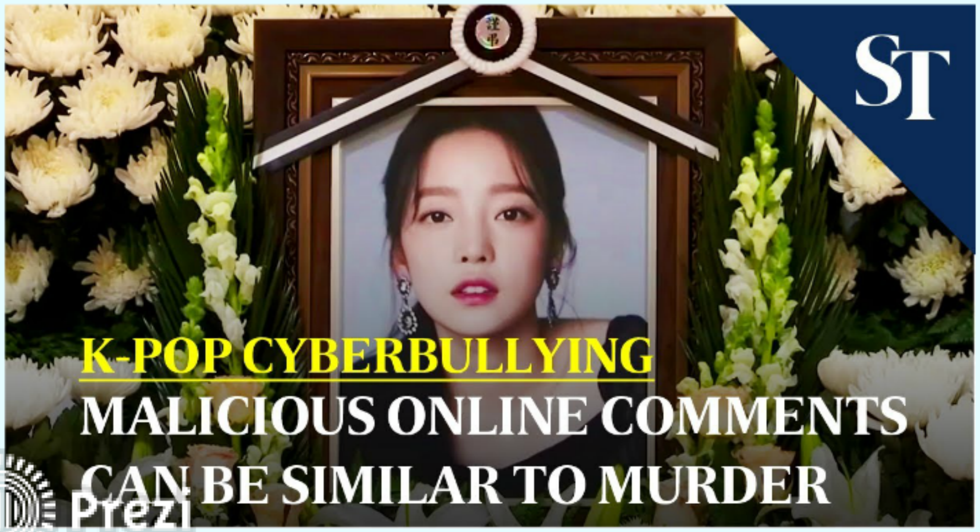
Cyberbullying real strories

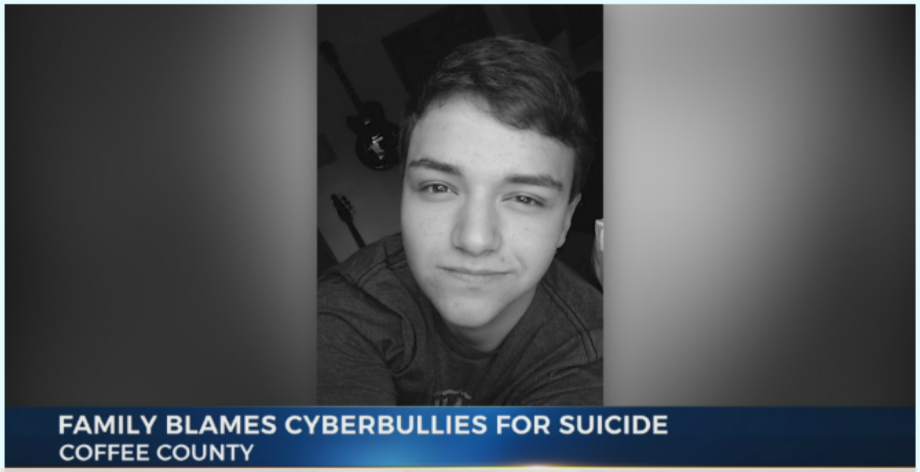


Barndy Vela's sister said that people made fake dating profiles of her sister.


NEWS ROOM
GIRLS SUSPECTED OF CYBER-BULLYING TEEN
Police: Rebecca Sedwick killed herself after being bullied
LIVE
CNN

Screenshots of “anonymous” comments made to Rebecca on Ask.fm, saying things like “Nobody cares about you” and “you seriously deserve to die.”

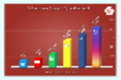




Channing Smith' family says his classmates posted a screenshot on Instagram and Snapchat of text messages between Channing and another boy.

CyberCrime

Cyber-Bullying



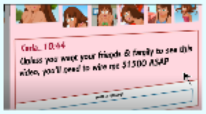
Cyberbullying real strories

[illegible]

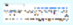
[illegible]

[illegible]

Cyber-Extortion



Carla, 10:44
Unless you want your friends & family to see this video, you'll need to wire me $1500 ASAP

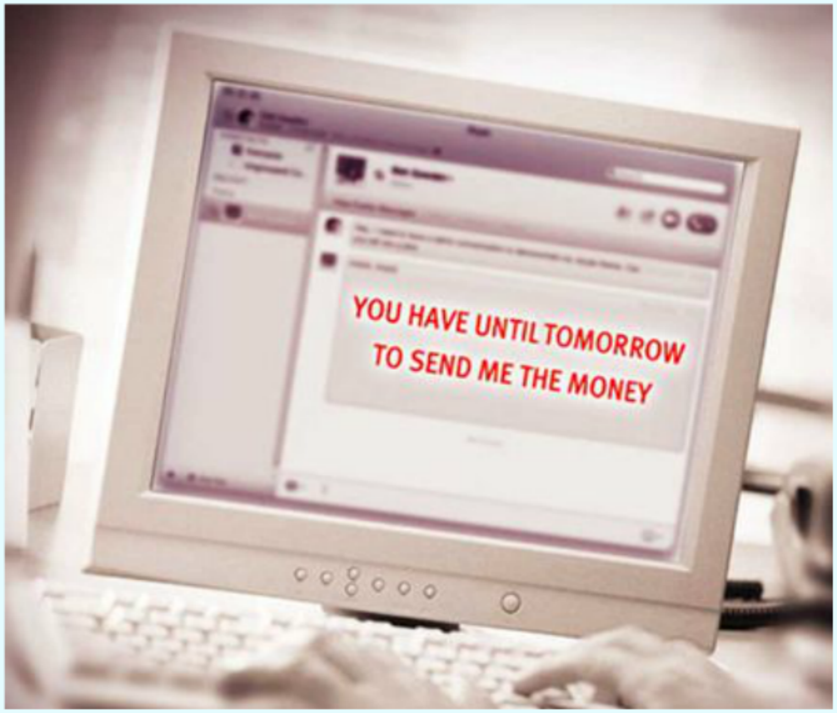


[illegible]

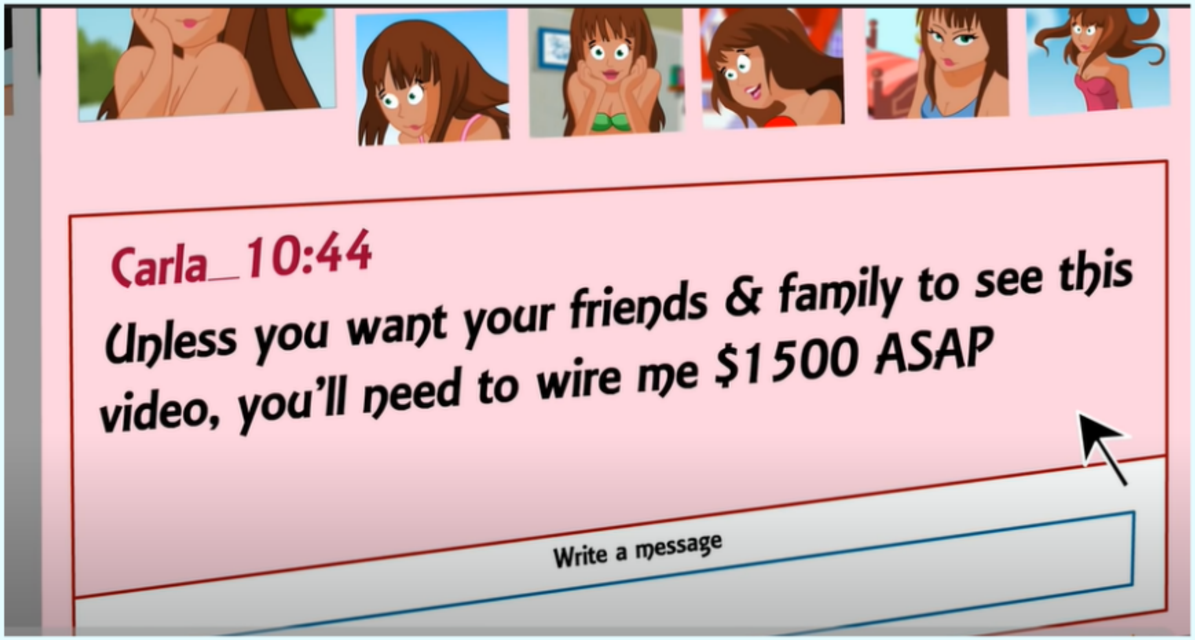
What to do?

[illegible]

Cyber-Extortion

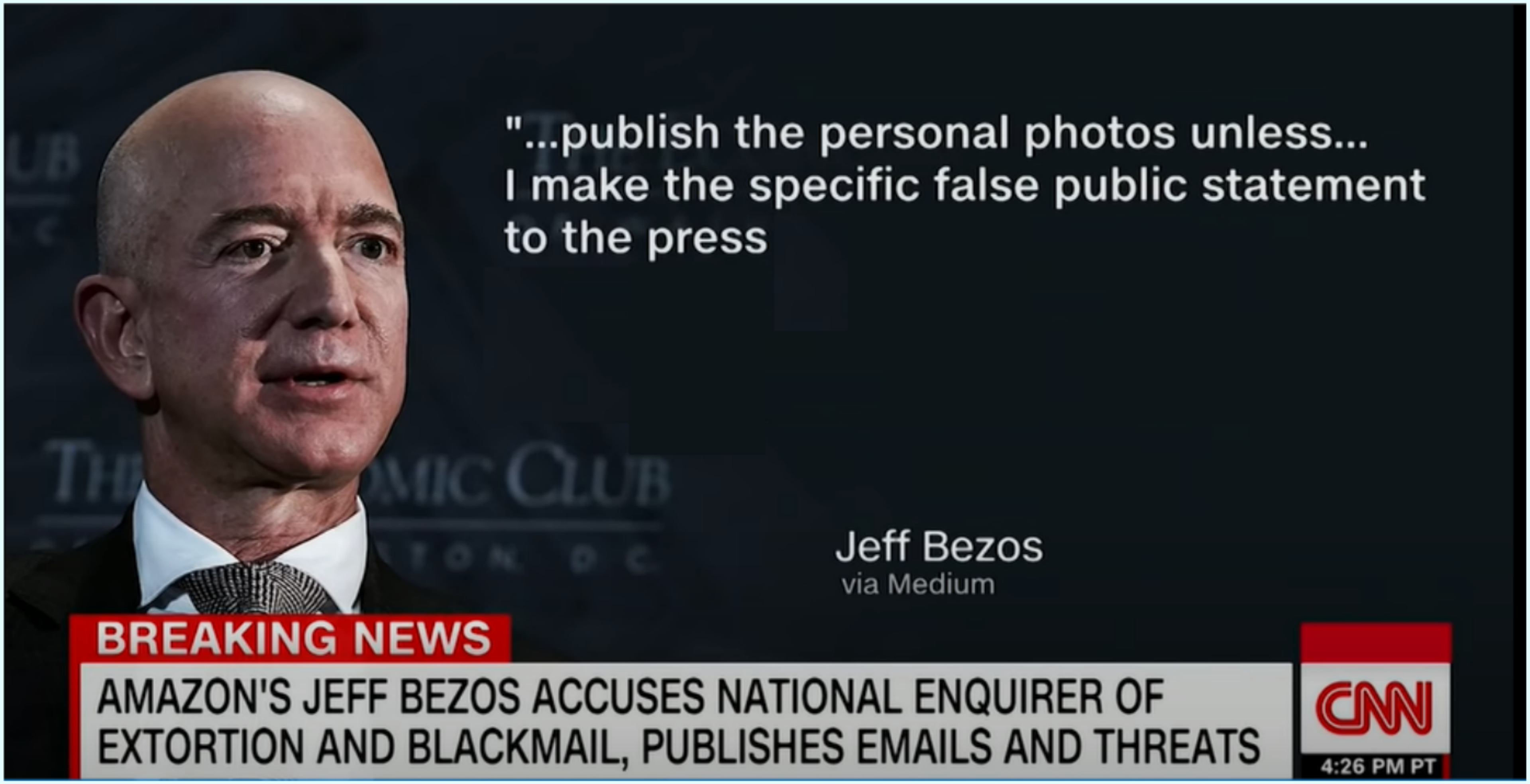


YOU HAVE UNTIL TOMORROW TO SEND ME THE MONEY



Carla_10:44

Unless you want your friends & family to see this video, you'll need to wire me $1500 ASAP

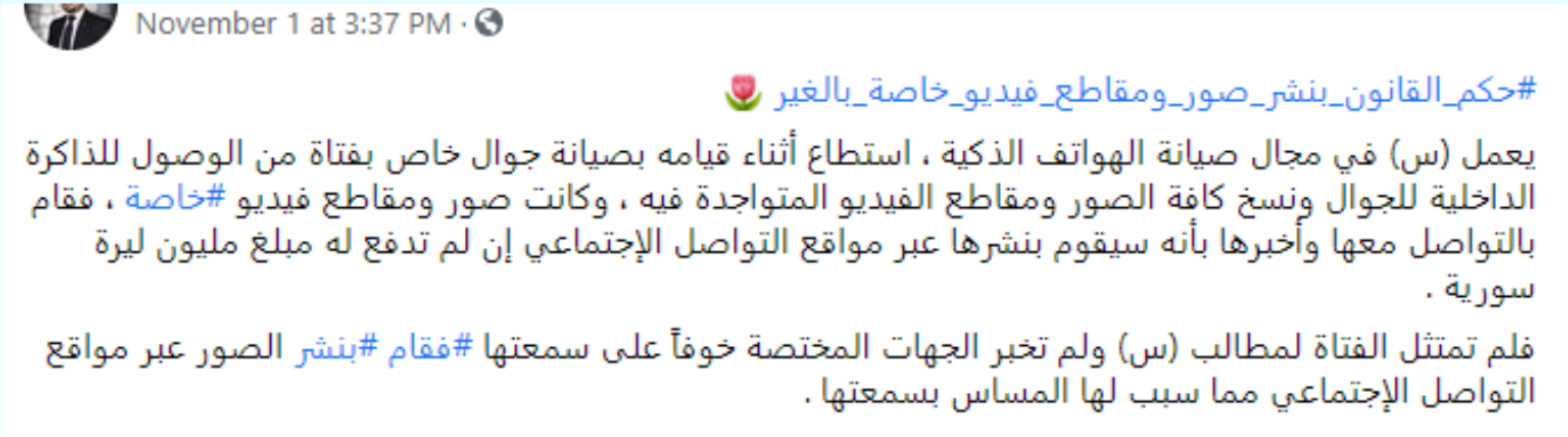


"...publish the personal photos unless...
I make the specific false public statement
to the press

Jeff Bezos
via Medium

BREAKING NEWS

AMAZON'S JEFF BEZOS ACCUSES NATIONAL ENQUIRER OF EXTORTION AND BLACKMAIL, PUBLISHES EMAILS AND THREATS



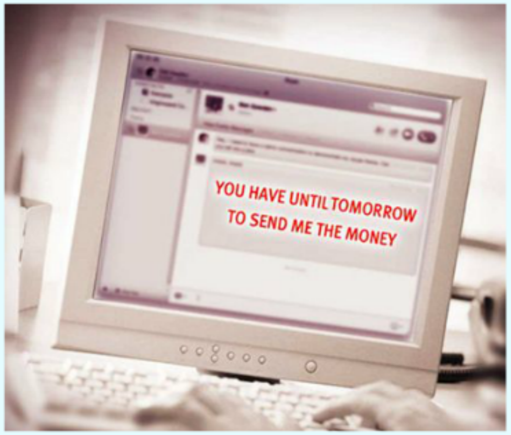
November 1 at 3:37 PM ·

#حكم_القانون_بنشر_صور_ومقاطع_فيديو_خاصة_بالغير 🌷

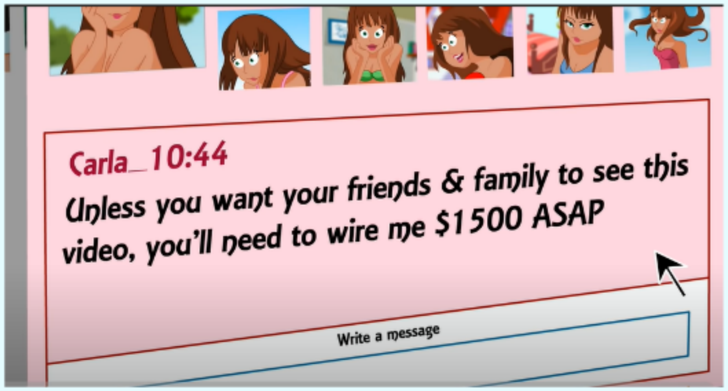
يعمل (س) في مجال صيانة الهواتف الذكية ، استطاع أثناء قيامه بصيانة جوال خاص بفتاة من الوصول للذاكرة الداخلية للجوال ونسخ كافة الصور ومقاطع الفيديو المتواجدة فيه ، وكانت صور ومقاطع فيديو #خاصة ، فقام بالتواصل معها وأخبرها بأنه سيقوم بنشرها عبر مواقع التواصل الإجتماعي إن لم تدفع له مبلغ مليون ليرة سورية .

فلم تمتثل الفتاة لمطالب (س) ولم تخبر الجهات المختصة خوفاً على سمعتها #فقام #بنشر الصور عبر مواقع التواصل الإجتماعي مما سبب لها المساس بسمعتها .

Cyber-Extortion

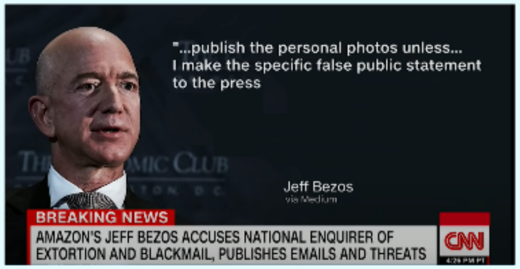


YOU HAVE UNTIL TOMORROW TO SEND ME THE MONEY



Carla_10:44

Unless you want your friends & family to see this video, you'll need to wire me $1500 ASAP



"...publish the personal photos unless... I make the specific false public statement to the press

Jeff Bezos
via Medium

BREAKING NEWS

AMAZON'S JEFF BEZOS ACCUSES NATIONAL ENQUIRER OF EXTORTION AND BLACKMAIL, PUBLISHES EMAILS AND THREATS

[illegible]

قانون التواصل على الشبكة ومكافحة الجريمة المعلوماتية

المادة 23 - المرسوم التشريعي 17 لعام 2012

انتهاك حرمة الحياة الخاصة ..

يعاقب بالحبس من شهر إلى ستة أشهر والغرامة من مئة ألف إلى خمسمئة ألف ليرة سورية كل من نشر
عن طريق الشبكة معلومات تنتهك خصوصية أي شخص دون رضاه حتى ولو كانت تلك المعلومات صحيحة .

What to do?

Don't keep information that you are ashamed of.

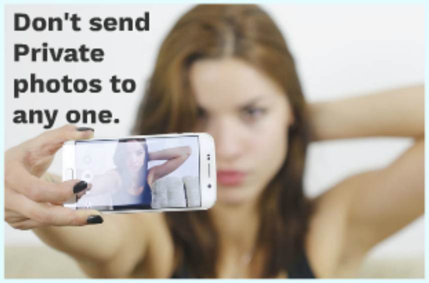
Don't send Private photos to any one.

- If someone threatens to share explicit images of you unless you pay them money:
  - Contact the police and provide evidence and screen shots.
  - Don't communicate further with the criminals.
  - Suspend you social media account.
  - Use the online reporting process to report the matter to Skype, YouTube etc.
  - Don't pay, they'll ask for more.

What to do?

No privacy on Internet

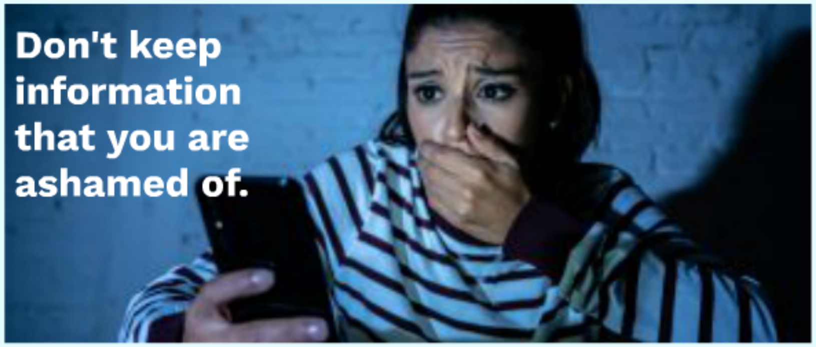
Don't keep information that you are ashamed of.

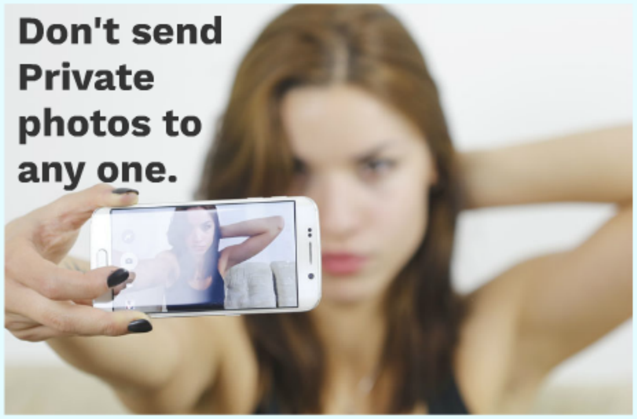

Don't send Private photos to any one.

- If someone threatens to share explicit images of you unless you pay them money:
  - Contact the police and provide evidence and screen shots.
  - Don't communicate further with the criminals.
  - Suspend you social media account.
  - Use the online reporting process to report the matter to Skype, YouTube etc.
  - Don't pay, they'll ask for more.

What to do?

No privacy on Internet


Don't keep information that you are ashamed of.

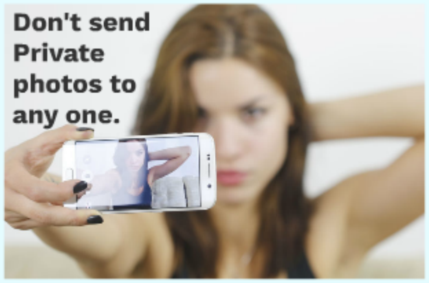

Don't send Private photos to any one.

someone threatens to share explicit images of you ur
u pay them money:

What to do?

No privacy on Internet

Don't keep information that you are ashamed of.



Don't send Private photos to any one.

- If someone threatens to share explicit images of you unless you pay them money:
  - Contact the police and provide evidence and screen shots.
  - Don't communicate further with the criminals.
  - Suspend you social media account.
  - Use the online reporting process to report the matter to Skype, YouTube etc.
  - Don't pay, they'll ask for more.

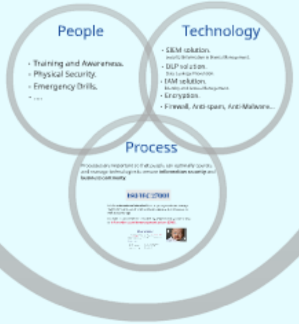
قانون التواصل على الشبكة ومكافحة الجريمة المعلوماتية

المادة 23 - المرسوم التشريعي 17 لعام 2012

انتهاك حرمة الحياة الخاصة ..

يعاقب بالحبس من شهر إلى ستة أشهر والغرامة من مئة ألف إلى خمسمئة الف ليرة سورية كل من نشر
عن طريق الشبكة معلومات تنتهك خصوصية أي شخصدون رضاه حتى ولو كانت تلك المعلومات صحيحة .

Countermeasures



People

- Training and Awareness.
- Physical Security.
- Emergency Drills.
- ...

Technology

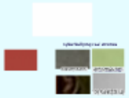
- SIEM solution.
- DLP solution.
- IAM solution.
- Encryption.
- Firewall, Anti-spam, Anti-Malware...

Process

ISO/IEC 27001

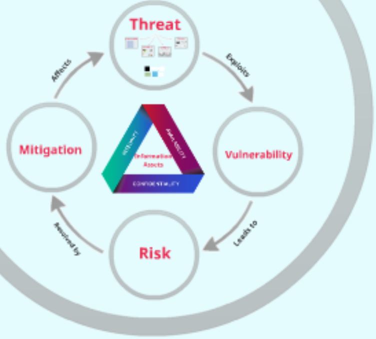
CyberCrime

Cyber-Bullying



Cyber-Extortion

Information Security



Threat

Exploits

Vulnerability

Leads to

Risk

Resolved by

Mitigation

Affects

INTEGRITY

AVAILABILITY

CONFIDENTIALITY

Information Assets

Agenda

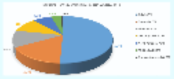
- Preface
- Information Security
- CyberSecurity Threats
- Countermeasures
- CyberCrime

Thank You

APPS

Information Communication Technology

Preface



Cyber-Attacks Statistics

CyberAttacks 2019-2020

Thank You

APPS

Information Communication Technology