

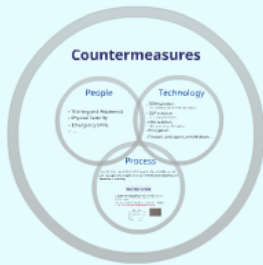
Information Security Awareness



Who are we?

IT company provides range of Information technology services

Business Solutions	IT Security Solutions and Services										
<ul style="list-style-type: none"> ERP Solutions Cloud Migration Services Business Process Automation Mobile Application Development 	<table border="1"> <thead> <tr> <th>Solution</th> <th>Service</th> </tr> </thead> <tbody> <tr> <td>CSM</td> <td>Information Management</td> </tr> <tr> <td>SIEM</td> <td>Operational Reporting</td> </tr> <tr> <td>UCM</td> <td>IT Security Policy Enforcement</td> </tr> <tr> <td>U2M</td> <td>Security Training Awareness</td> </tr> </tbody> </table>	Solution	Service	CSM	Information Management	SIEM	Operational Reporting	UCM	IT Security Policy Enforcement	U2M	Security Training Awareness
Solution	Service										
CSM	Information Management										
SIEM	Operational Reporting										
UCM	IT Security Policy Enforcement										
U2M	Security Training Awareness										



Information Security Awareness



Who are we?

IT company provides range of Information technology services

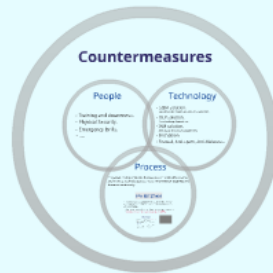
Business Solutions

ERP Solution
 Management system solution designed for a
 company's financial, human resources, customer relationship
 management, supply chain management and other business
 processes.
Mobile App Building/Development
 An open development platform for building apps for mobile
 devices.

IT Security Solutions and Services

Solutions:
 - IDS
 - IPS
 - EDR
 - SIEM

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





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



Who are we?

IT company provides range of Information technology services

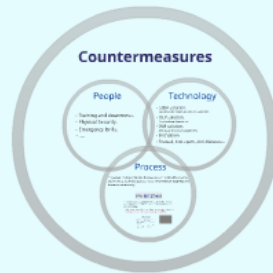
Business Solutions

ERP Solution
 Management systems - custom designed for the client's business
 - Financials, HR, Sales, Inventory, Production, Customer Relationship Management, Supply Chain Management, Project Management, CRM, HRM, etc.
Mobile App Building/Development
 For custom designed solutions for mobile devices, including Android and iOS.

IT Security Solutions and Services

Solutions:
 - IDS
 - IPS
 - SIEM
 - SIEM
 - SIEM

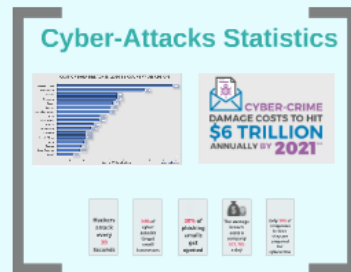
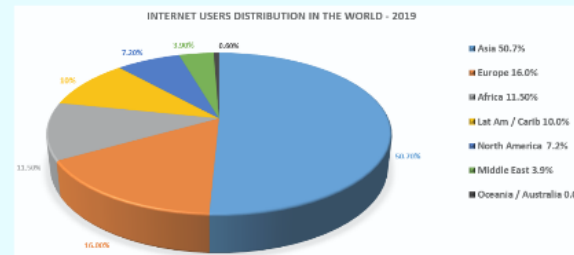
Services:
 - Network Security Assessment
 - Incident Response
 - IT Security Policy Development
 - Security Training and Awareness



Agenda

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

Preface

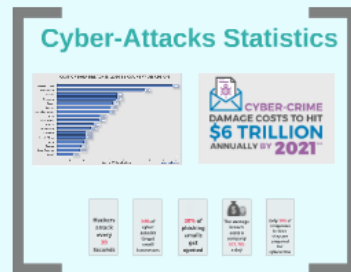
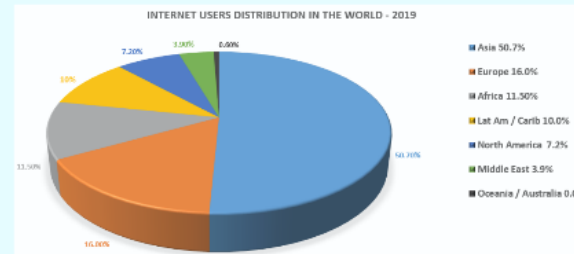


2020 *This Is What Happens In An Internet Minute*

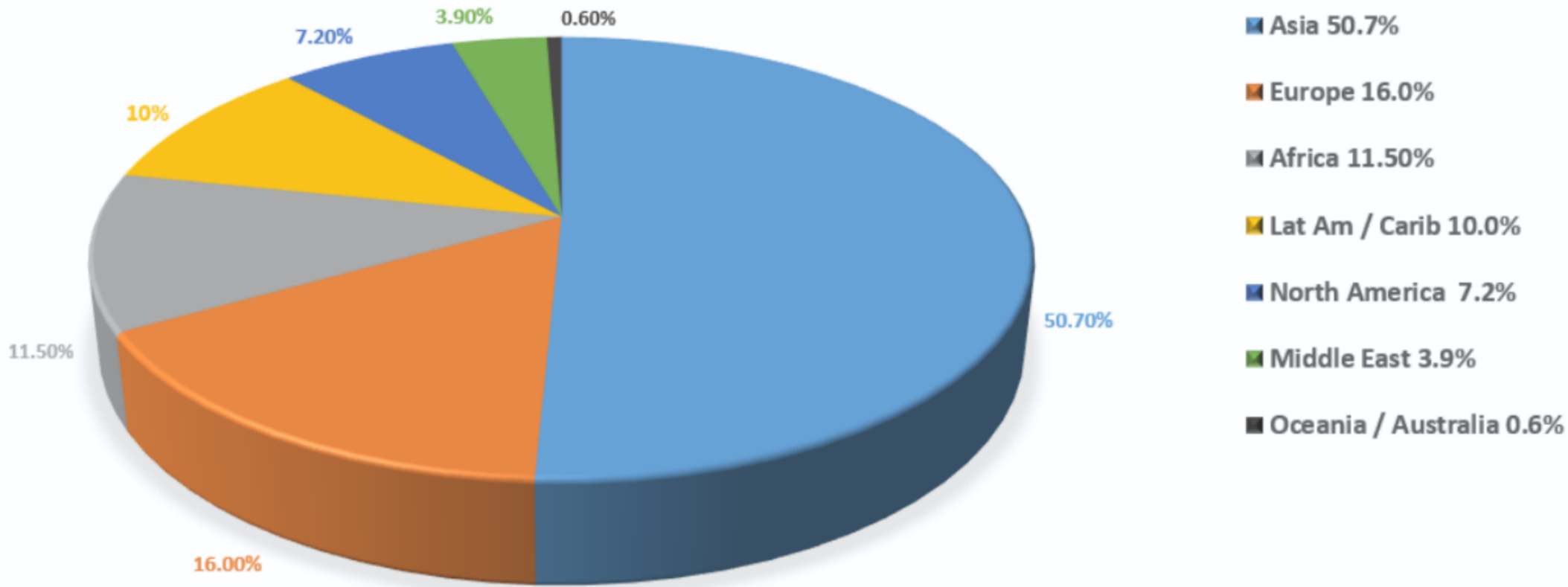


Created By:
@LoriLewis
@OfficiallyChadd

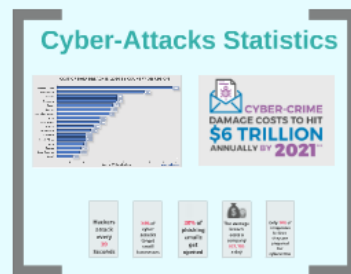
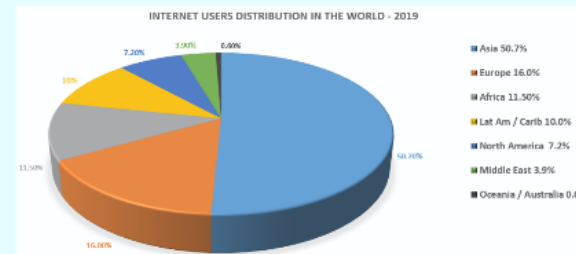
Preface



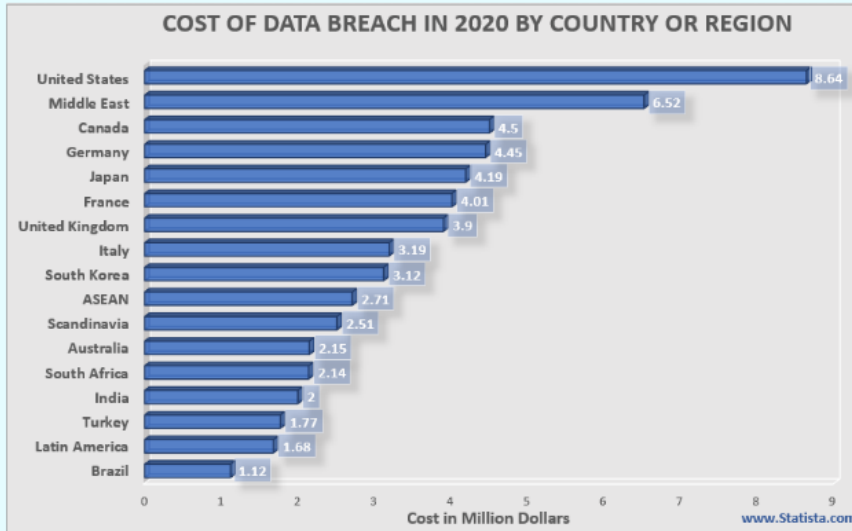
INTERNET USERS DISTRIBUTION IN THE WORLD - 2019



Preface



Cyber-Attacks Statistics



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

Hackers attack every 39 Seconds

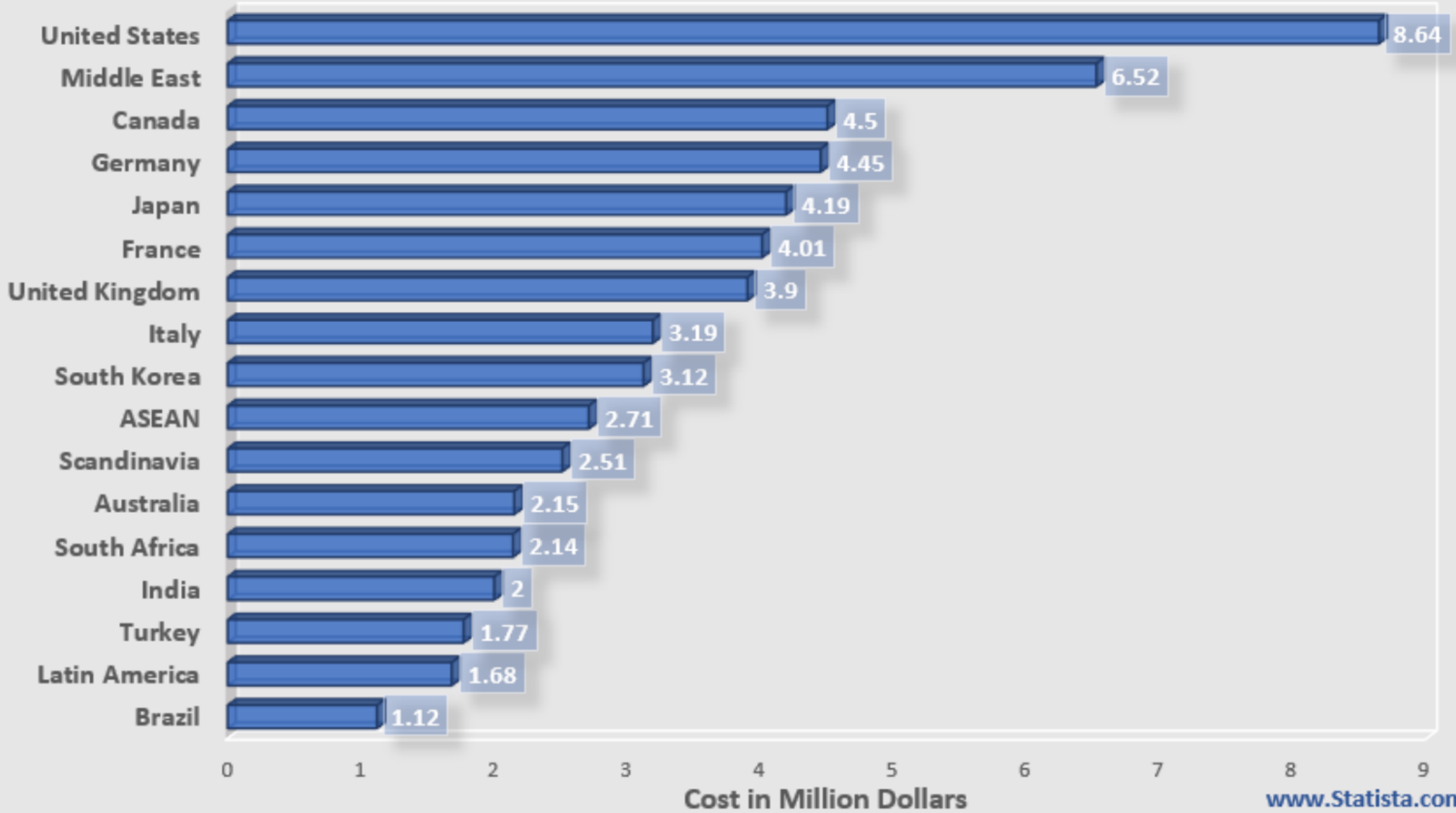
34% of cyber attacks target small businesses

30% of phishing emails get opened

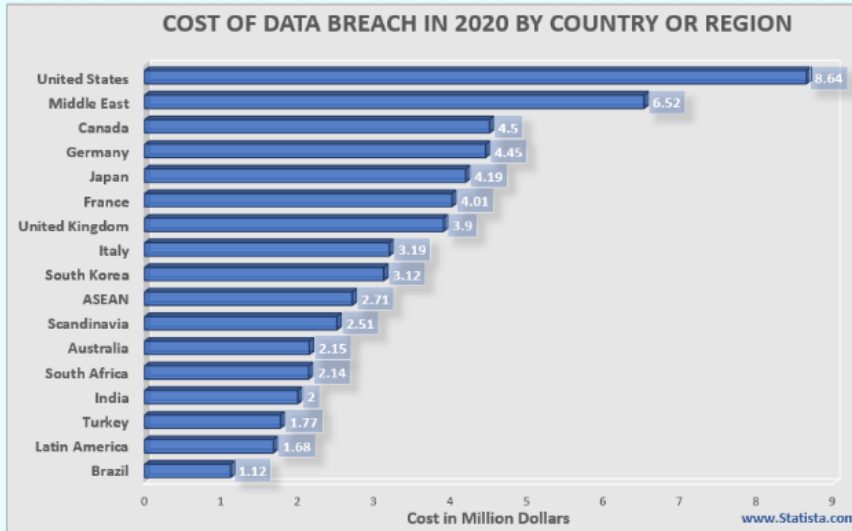
The average breach costs a company \$21,155 a day

Only 14% of companies believe they are prepared for cybercrime

COST OF DATA BREACH IN 2020 BY COUNTRY OR REGION



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

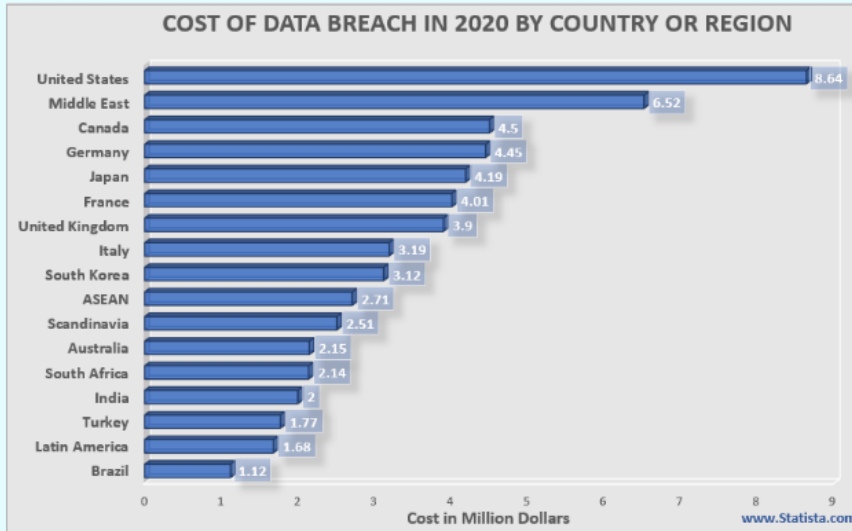


Only **14%** of
companies
believe
they are
prepared
for
cybercrime



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

1.77

1.68

2 3 4 5 6 7 8 9
Cost in Million Dollars www.Statista.com

ANNUALLY BY 20



Hackers
attack
every
39
Seconds



34% of
cyber
attacks
target
small
businesses



30% of
phishing
emails
get
opened

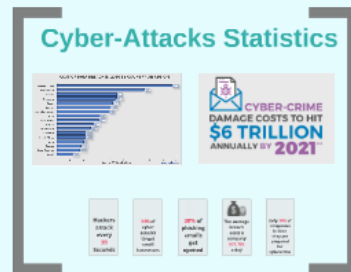
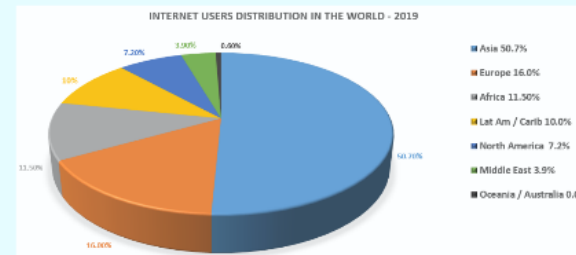


The average
breach
costs a
company
\$21,155
a day



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

Preface



CyberAttacks 2019-2020

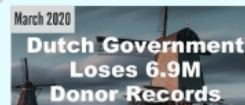


Marriott reveal its second customer data breach in **two years**.

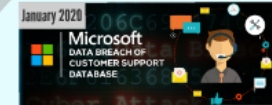
5.2 Million Guests affected according to CBC News.

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
------------------------	------------------------	--	--------------------------------------



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



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**

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



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



- 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

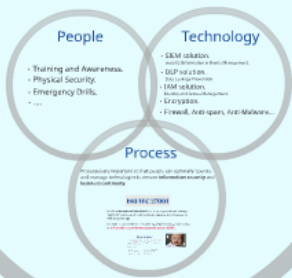
AMADEUS
Leisure Platform

Used by popular Israeli online travel booking services

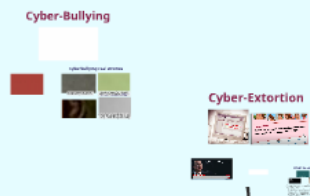
The leaked database contains:

- 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

Countermeasures



CyberCrime



Information Security



Agenda

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

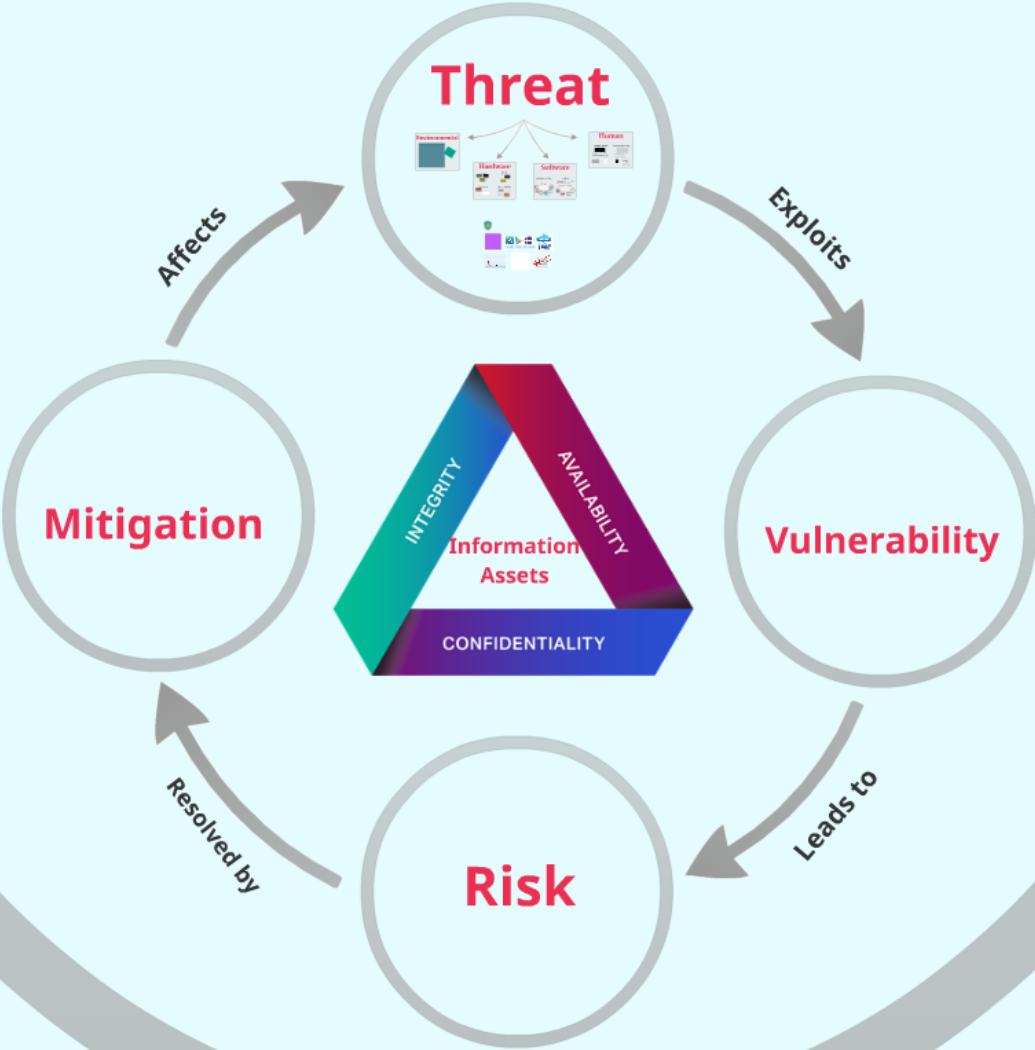
Thank You

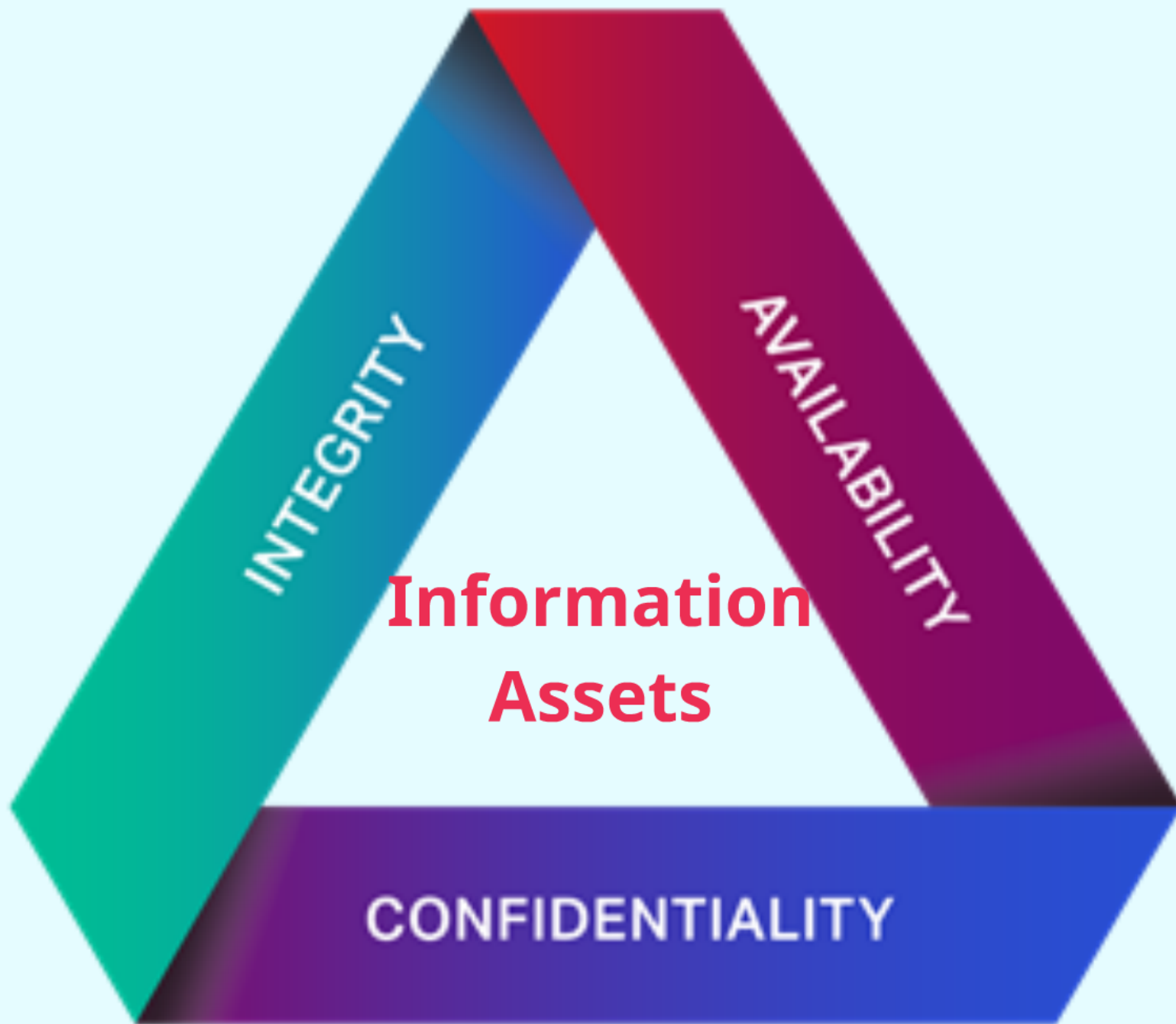


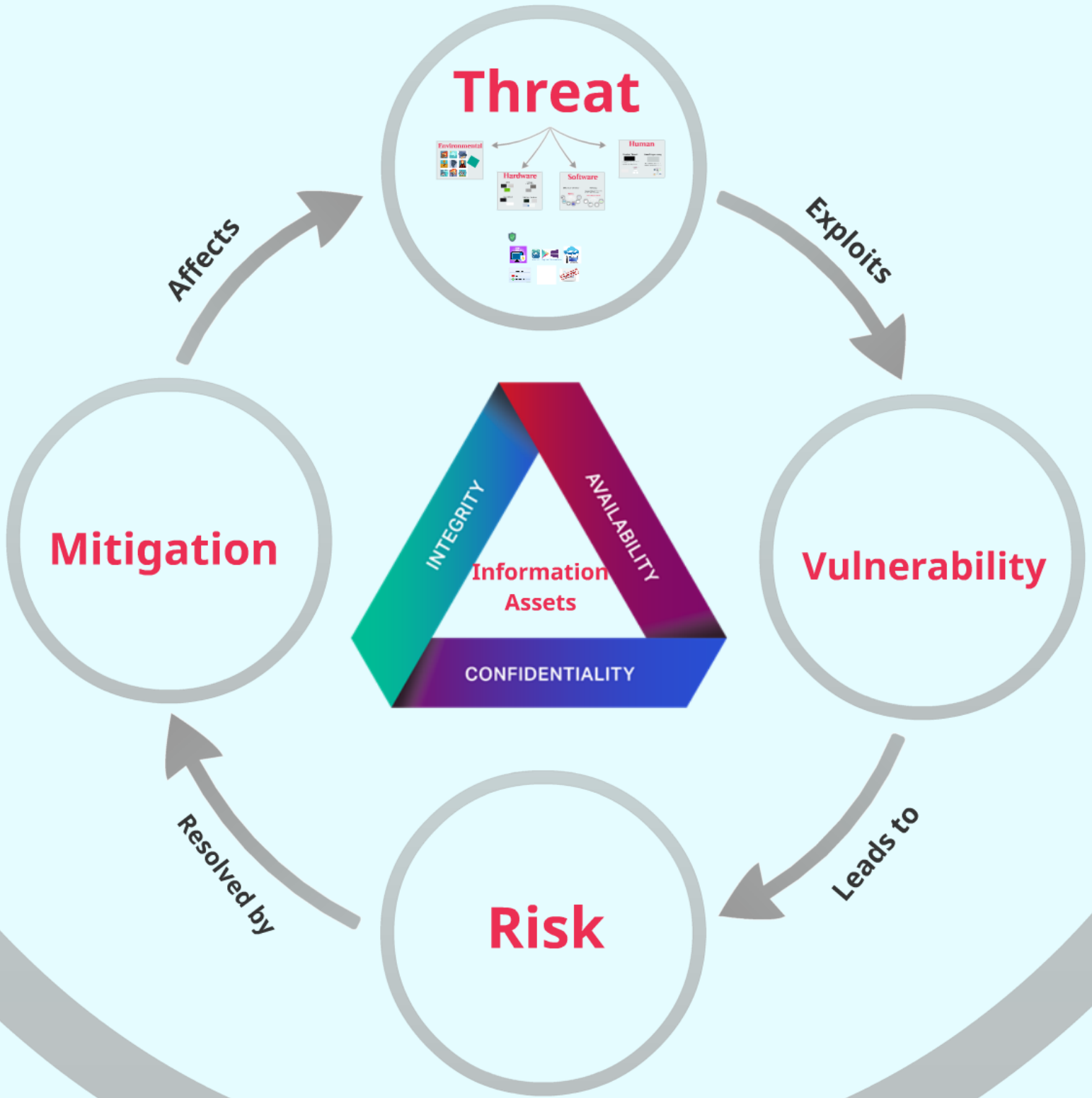
Preface



Information Security



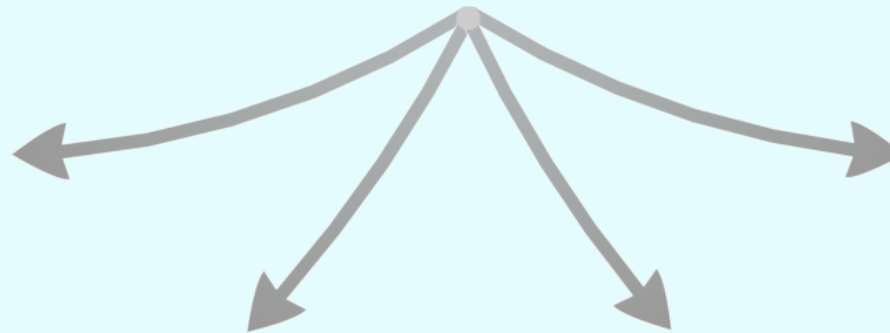




Threat

Environmental

5%



Hardware

Loss

Damage

Power Failure

Malicious Hardware

Software

Malicious software

Malware

Hacking

Common Hacking Techniques

Human

Insider Threat

Social Engineering



Environmental

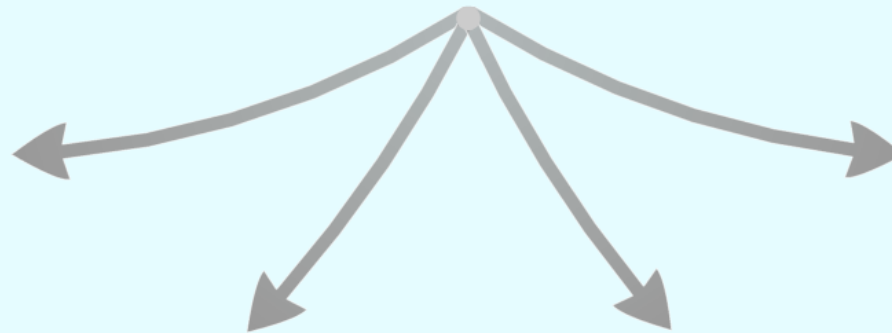


5%

Threat

Environmental

5%



Hardware

- Loss
- Damage
- Power Failure
- Malicious Hardware

Software

- Malicious software
 - Malware
- Hacking
 - 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



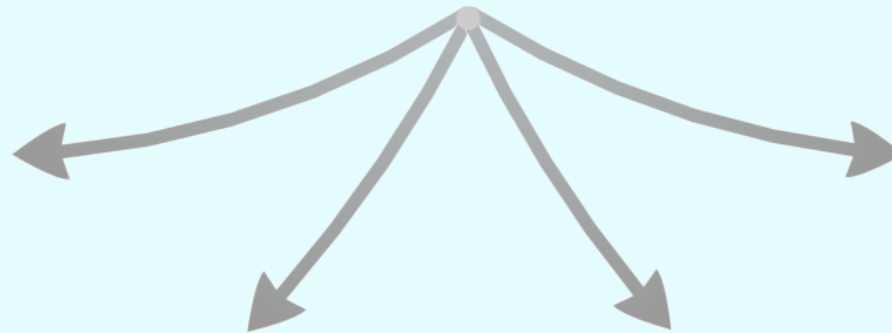
Malicious Hardware



Threat

Environmental

5%



Hardware

- Loss
- Damage
- Power Failure
- Malicious Hardware

Software

- Malicious software
 - Malware
- Hacking
 - Common Hacking Techniques

Human

- Insider Threat
- Social Engineering



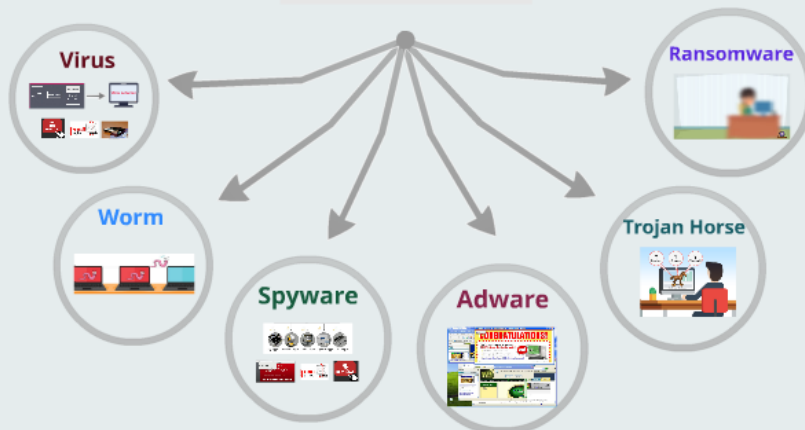
Software

Malicious software

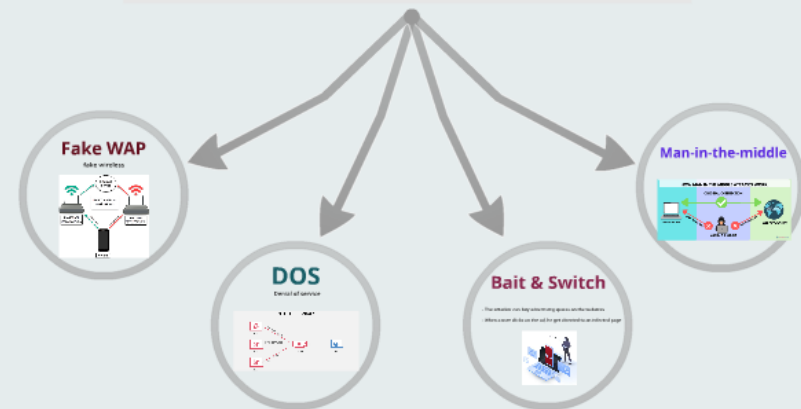
Hacking

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

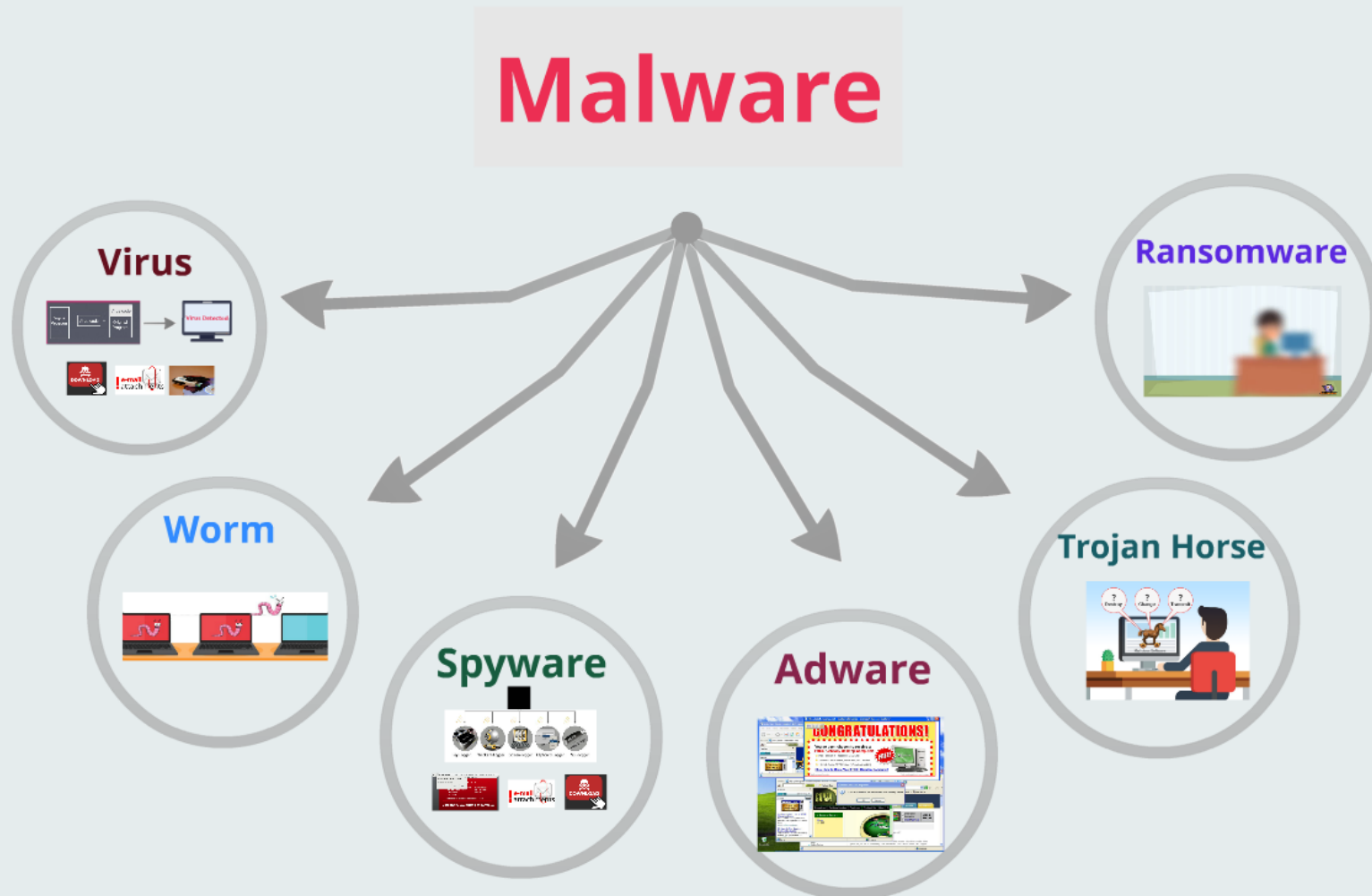
Malware



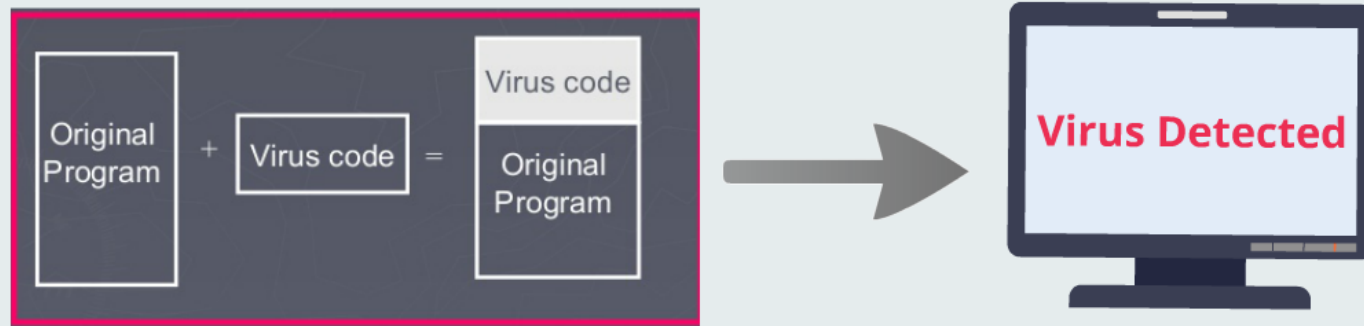
Common Hacking Techniques



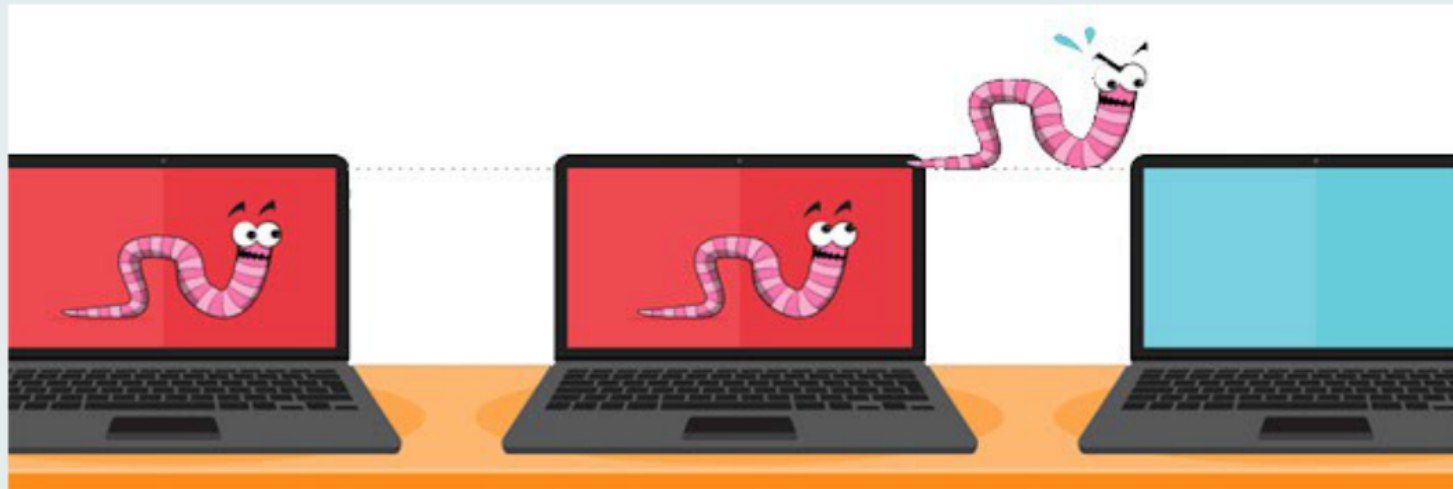
Malicious software



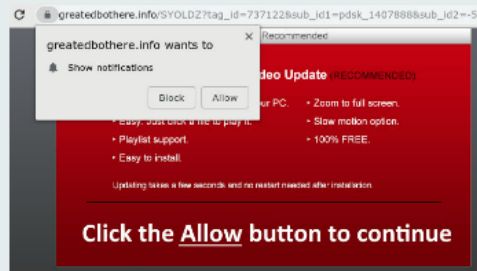
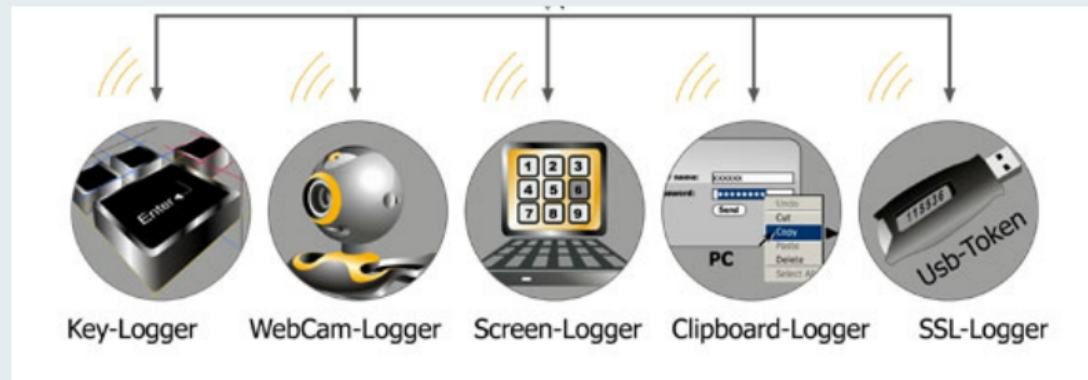
Virus



Worm



Spyware



Adware



Trojan Horse



Ransomware





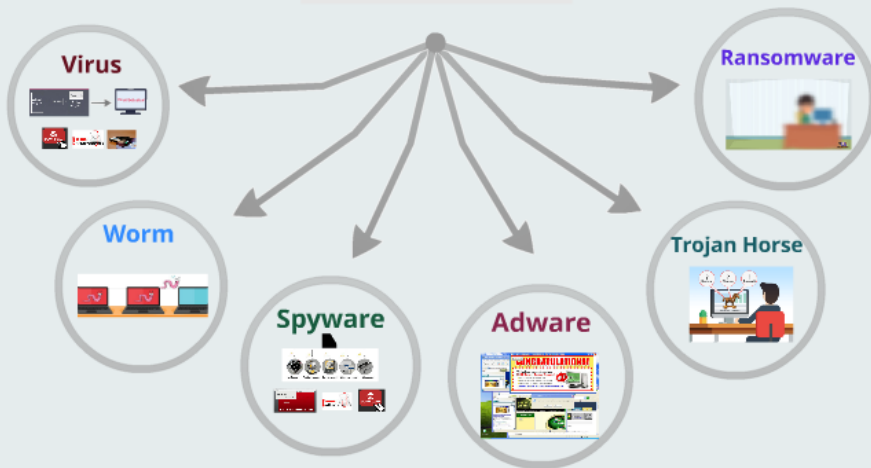
Software

Malicious software

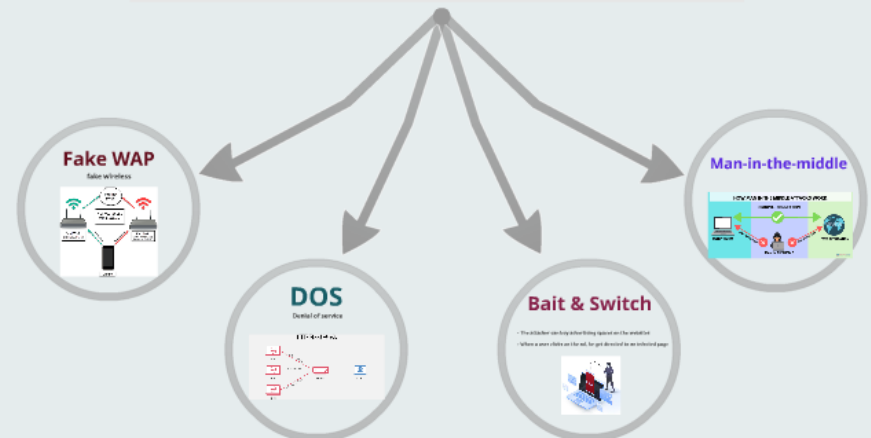
Hacking

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

Malware



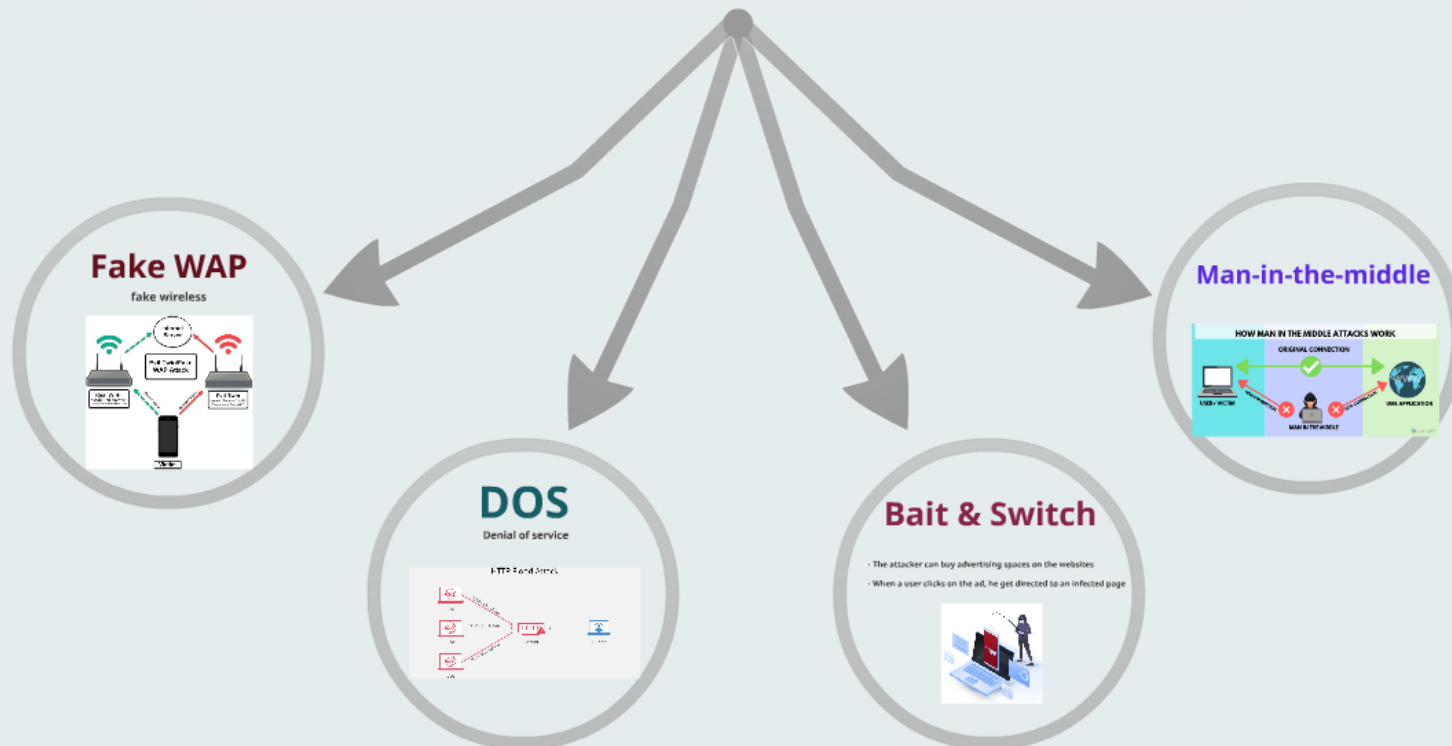
Common Hacking Techniques



Hacking

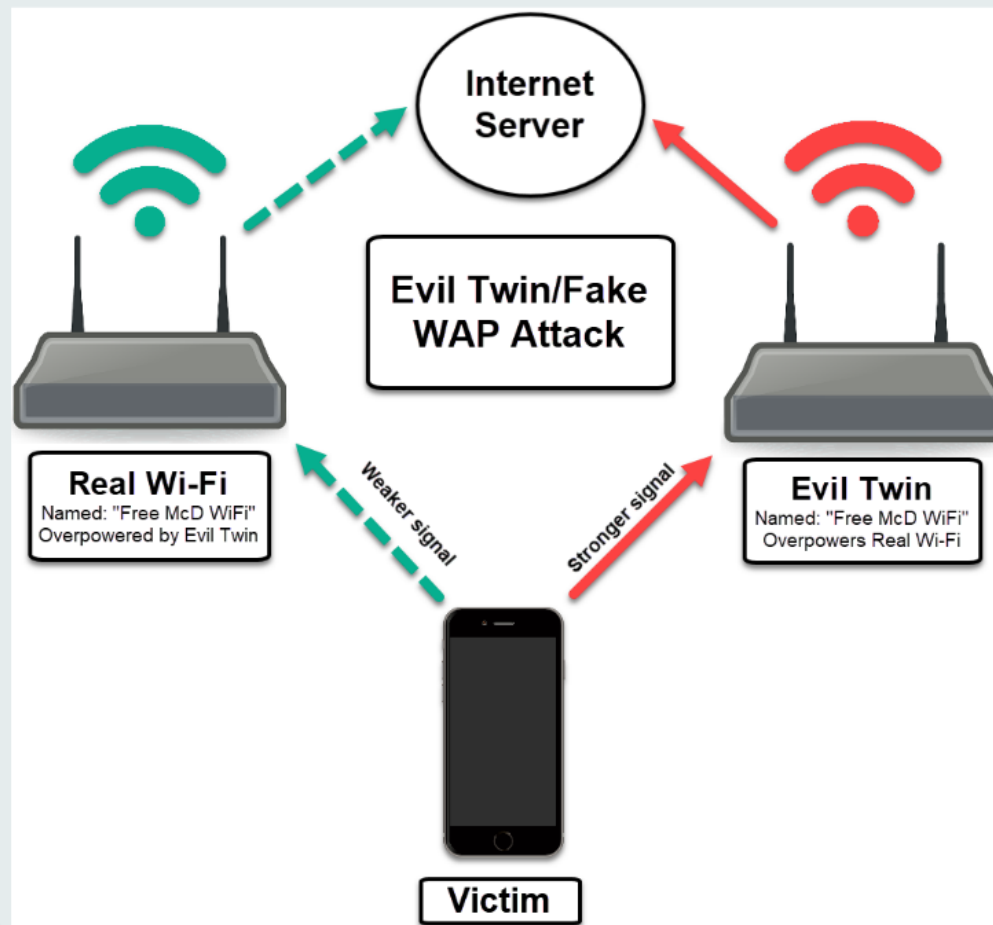
- Illegal access to an information system (computer, network ...) and obtaining or modifying data
- Hackers exploit weaknesses in information systems

Common Hacking Techniques



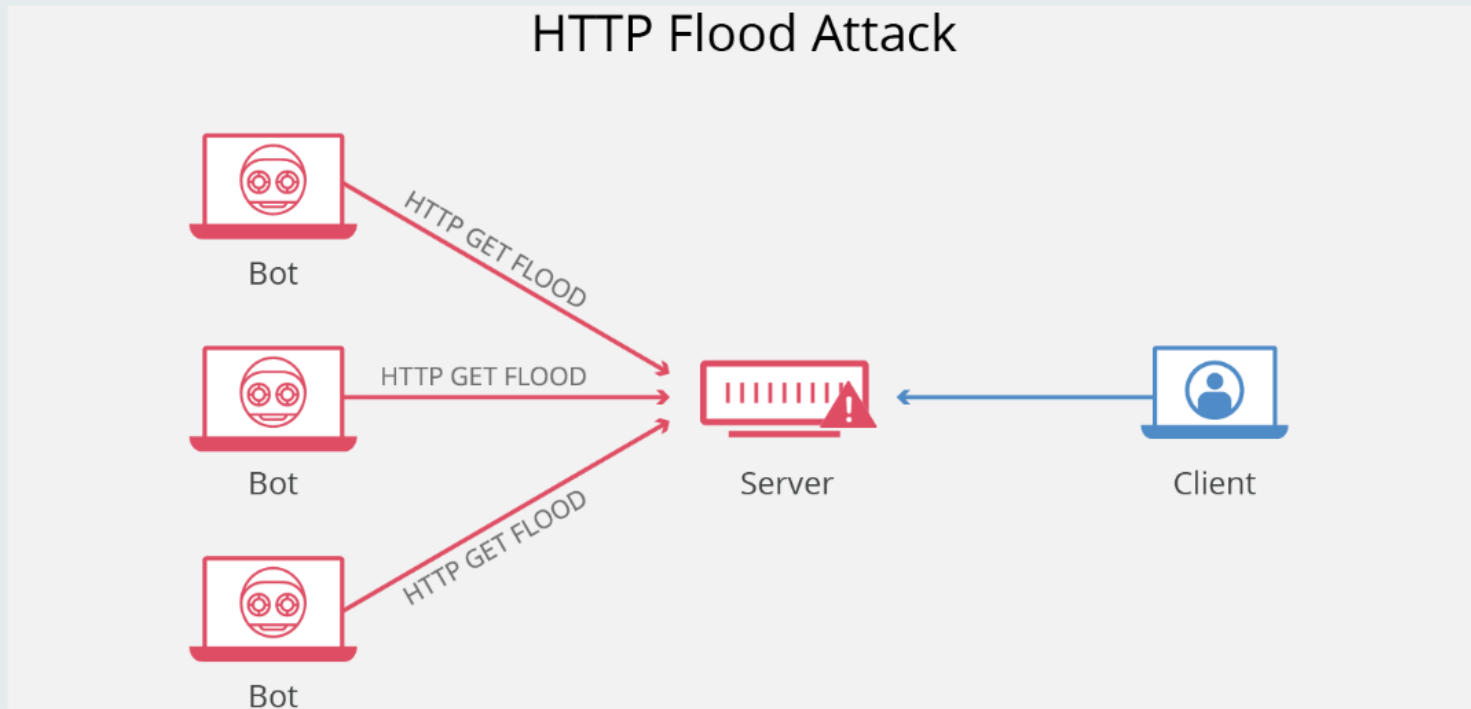
Fake WAP

fake wireless



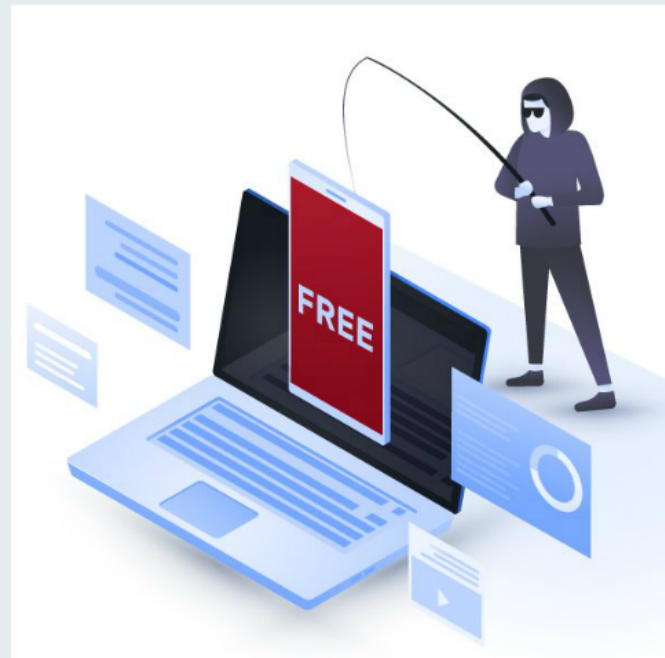
DOS

Denial of service

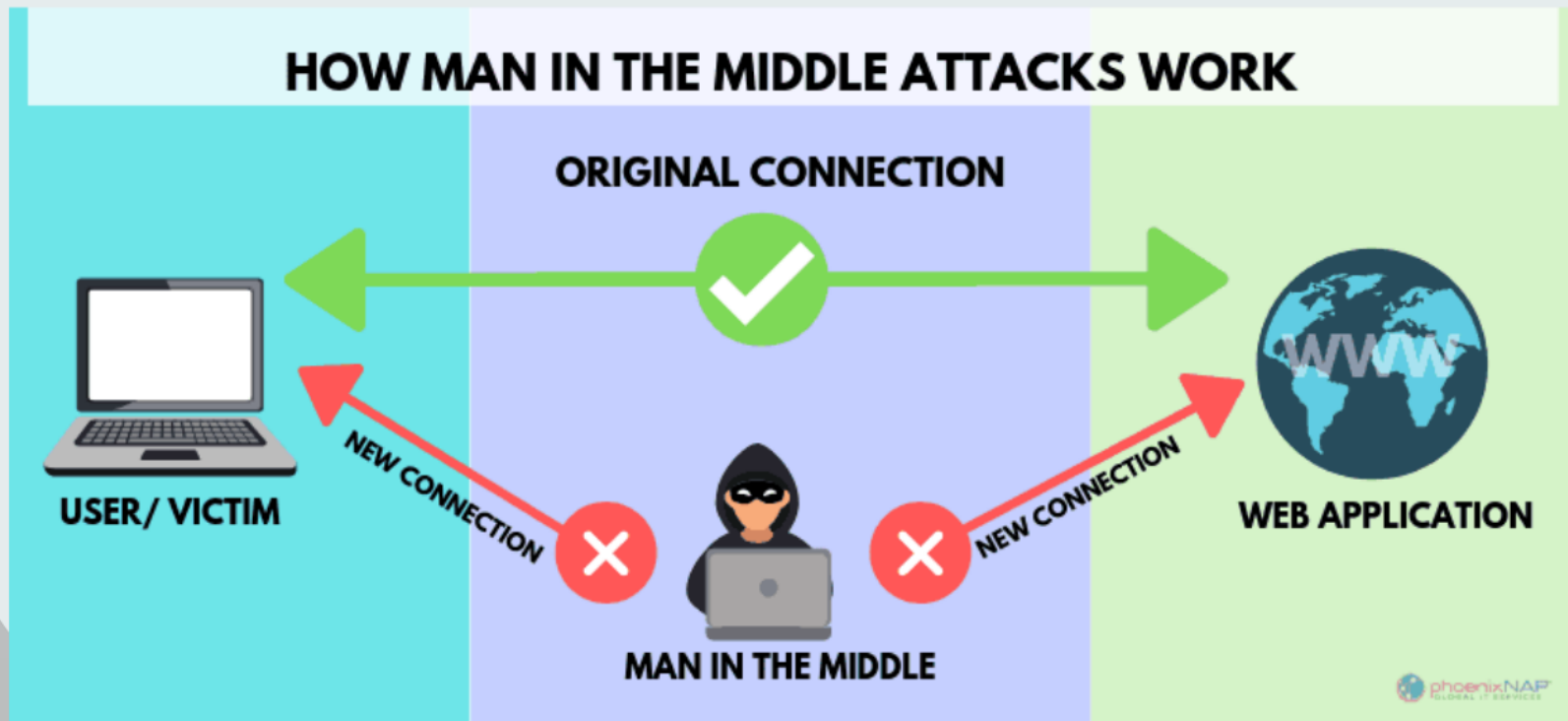


Bait & Switch

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



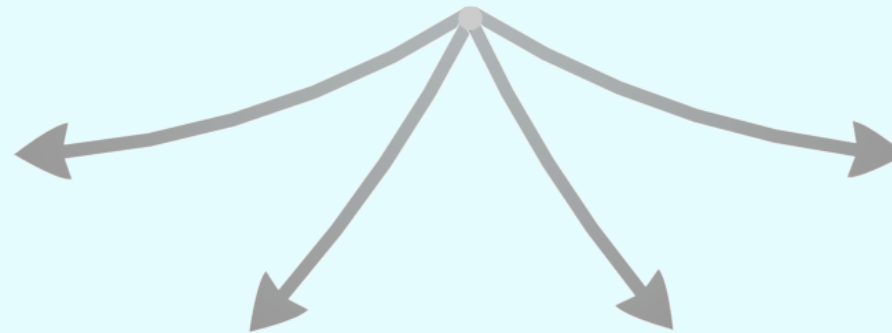
Man-in-the-middle



Threat

Environmental

5%



Hardware

Loss

Damage

Power Failure

Malicious Hardware

Software

Malicious software

Malware

Hacking

Illegal access to or tampering with computer resources...
Has been explicitly prohibited in software licenses.

Common Hacking Techniques

Human

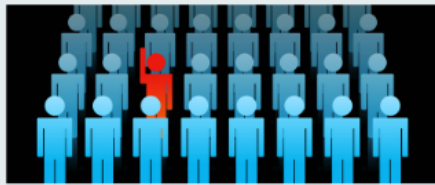
Insider Threat

Social Engineering



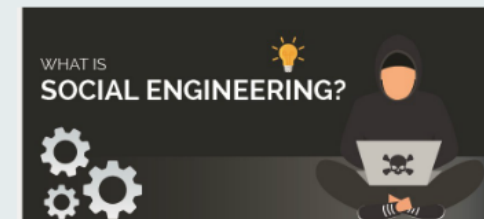
Human

Insider Threat

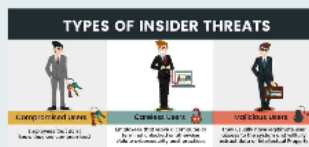


- Malicious activity against an organization, from people within the organization
- The usual suspects are employees or contractors with access to an organization's network, applications or databases

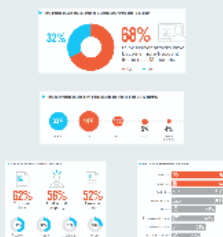
Social Engineering



- 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



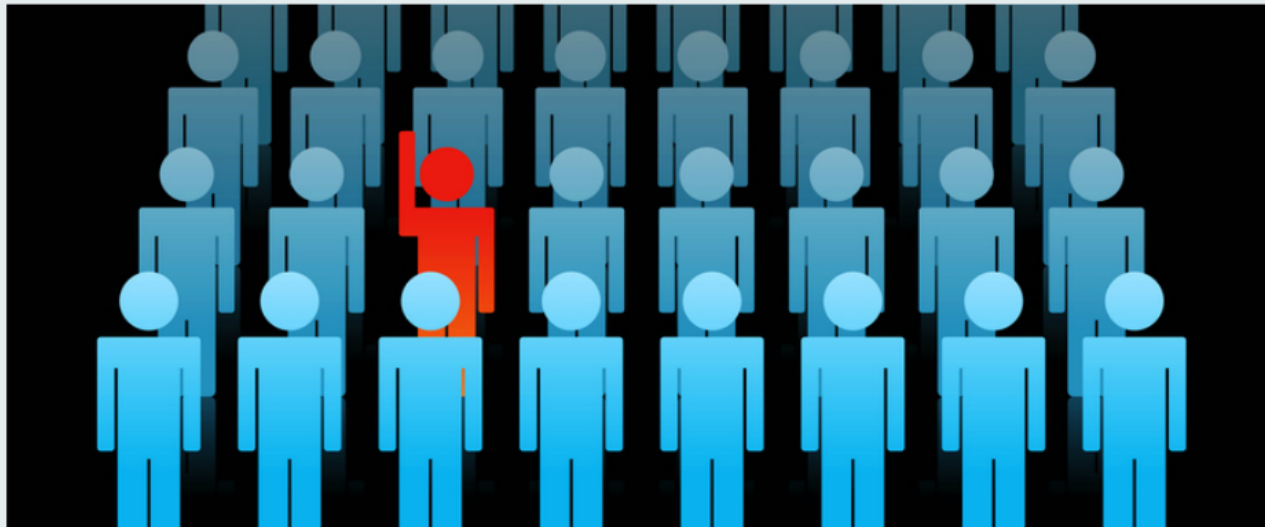
Insider threats report for 2019
Source: cybersecurity-insiders.com



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



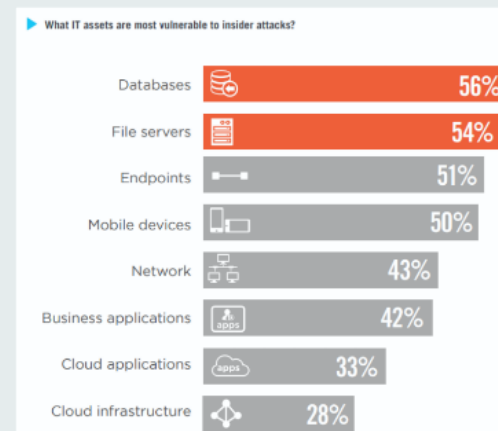
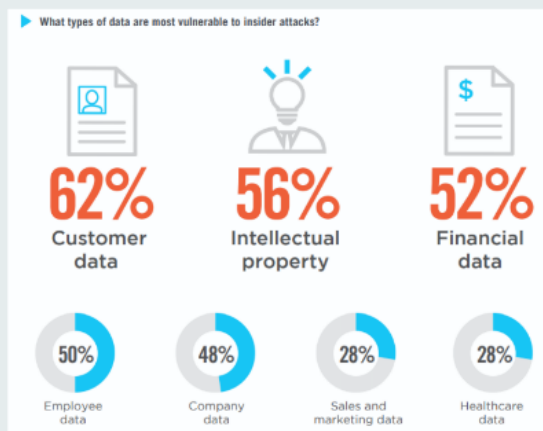
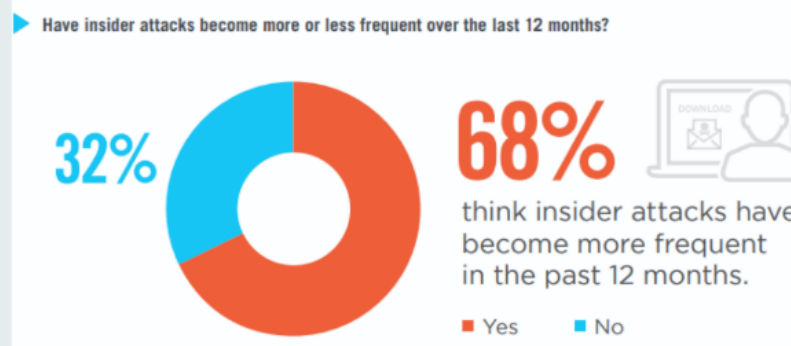
Malicious Users



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



Source: [cybersecurity-insiders.com](https://www.cybersecurity-insiders.com)

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

32%



68%



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

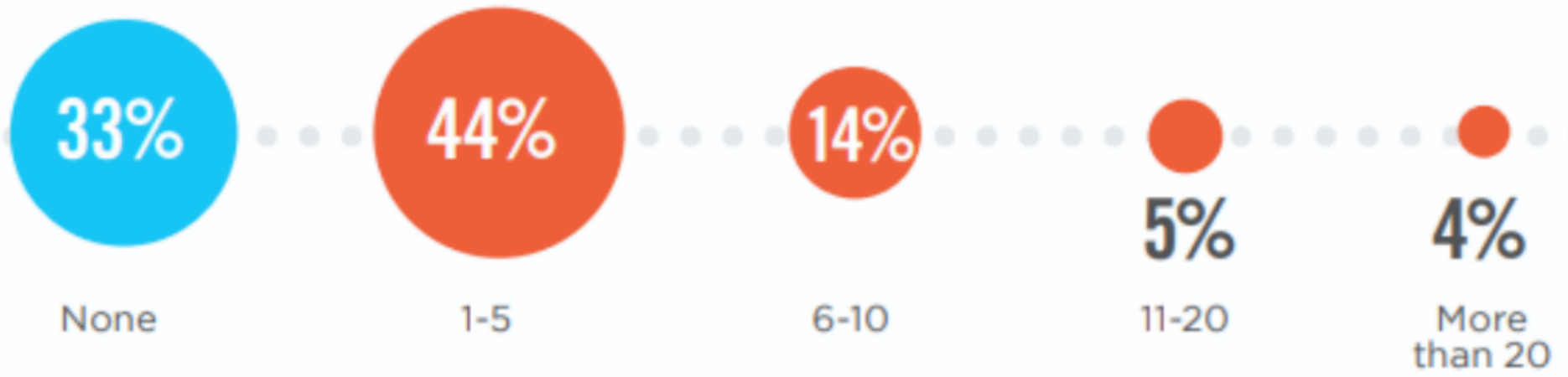
■ Yes

■ No

■ Yes

■ No

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



What are the most common causes of insider attacks?



▶ What IT assets are most vulnerable to insider attacks?

▶ What types of data are most vulnerable to insider attacks?



62%

Customer
data



56%

Intellectual
property



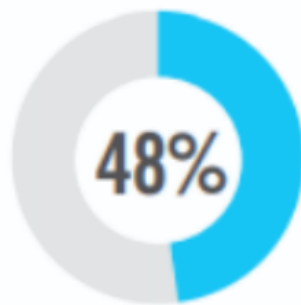
52%

Financial
data



50%

Employee
data



48%

Company
data



28%

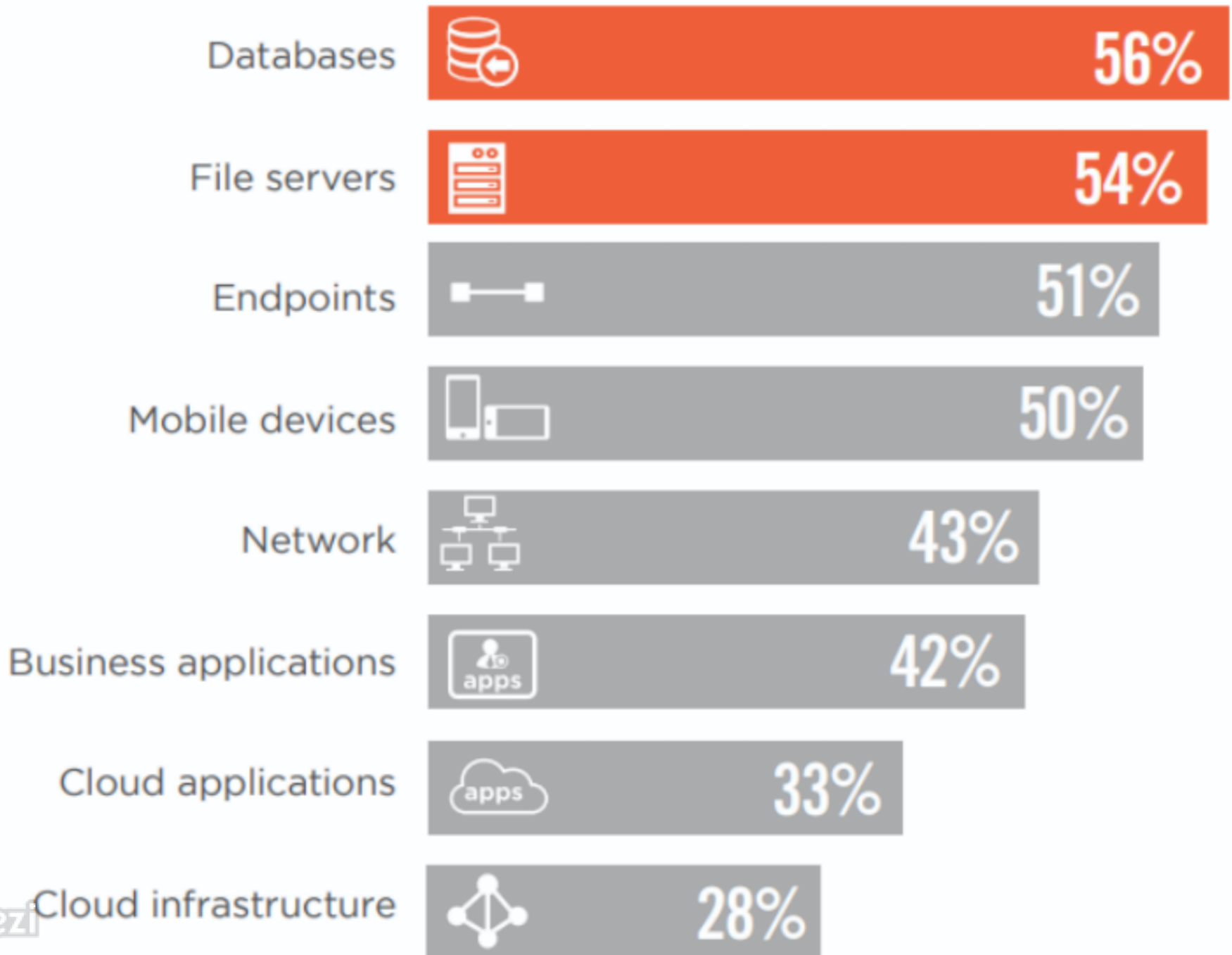
Sales and
marketing data



28%

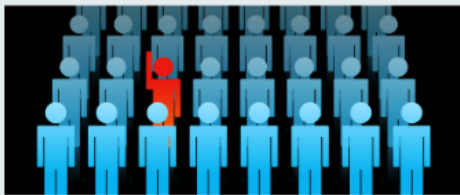
Healthcare
data

▶ What IT assets are most vulnerable to insider attacks?



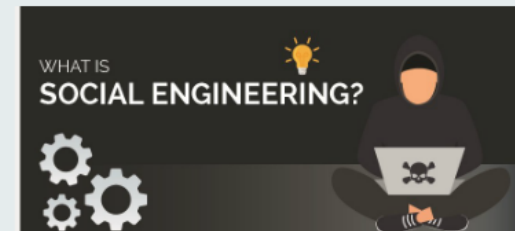
Human

Insider Threat



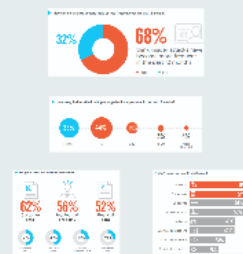
- Malicious activity against an organization, from people within the organization
- The usual suspects are employees or contractors with access to an organization's network, applications or databases

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

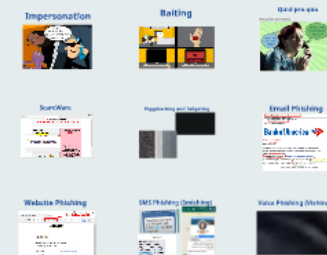
Insider threats report for 2019
Source: cybersecurityinsiders.com



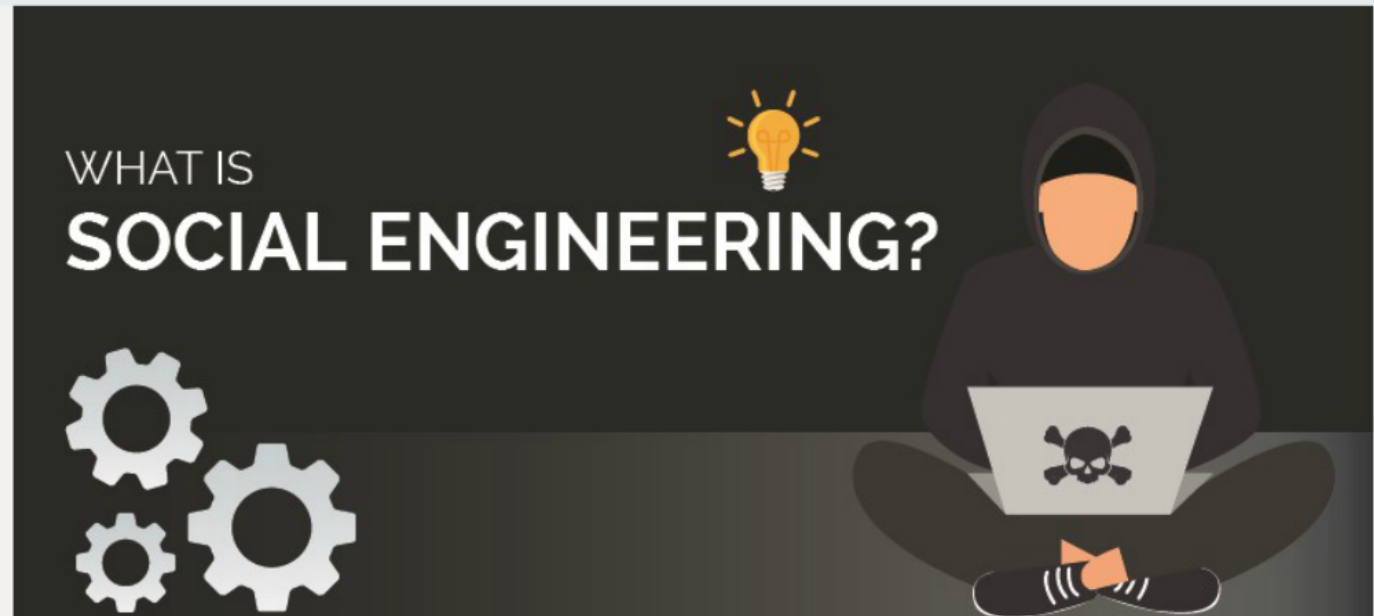
Phases in a Social Engineering Attack



Social Engineering Techniques



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



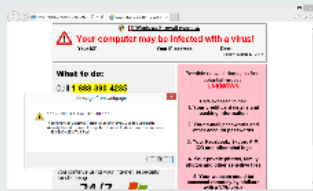
Baiting



Quid pro quo



ScareWare



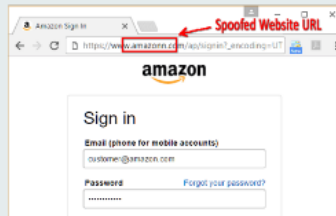
Piggybacking and Tailgating



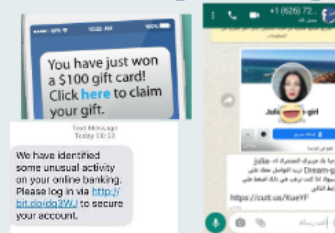
Email Phishing



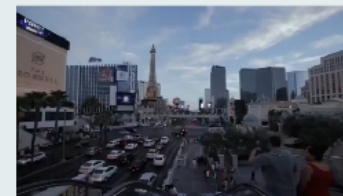
Website Phishing



SMS Phishing (Smishing)



Voice Phishing (Vishing)



Impersonation



Baiting



Quid pro quo

Means something for something:



ScareWare

The screenshot shows a web browser window with the address bar containing `http://alert.windows.com.co...` and a tab titled "WARNING - SECURITY ALERT". The main content area features a large warning box with a red triangle icon and the text: **(1) Windows Firewall warning: Your computer may be infected with a virus!** Below this, it lists "Your ISP:", "Your IP address:", and "Date: Tuesday, March 17, 2015".

To the left, a "What to do:" section instructs the user to "Call **1-888-390-4235**".

A pop-up window titled "Message from webpage" is overlaid on the page. It contains a yellow warning icon and the text: ***** 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). An "OK" button is at the bottom right of the pop-up.

On the right side of the page, a pink box lists "Possible network damages from potential viruses: **UNKNOWN**". Below this, it states "Data exposed to risk:" followed by a numbered list:

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

At the bottom of the page, there is a date "24/7" and a Windows logo.

Piggybacking and Tailgating



Email Phishing

From: Bank of America <crvdqi@comcast.net>

Subject: Notification Irregular Activity

Date: September 23, 2014 3:44:42 PM PDT

To: Undisclosed recipients: ;

Reply-To: crvdqi@comcast.net

Bank of America



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.

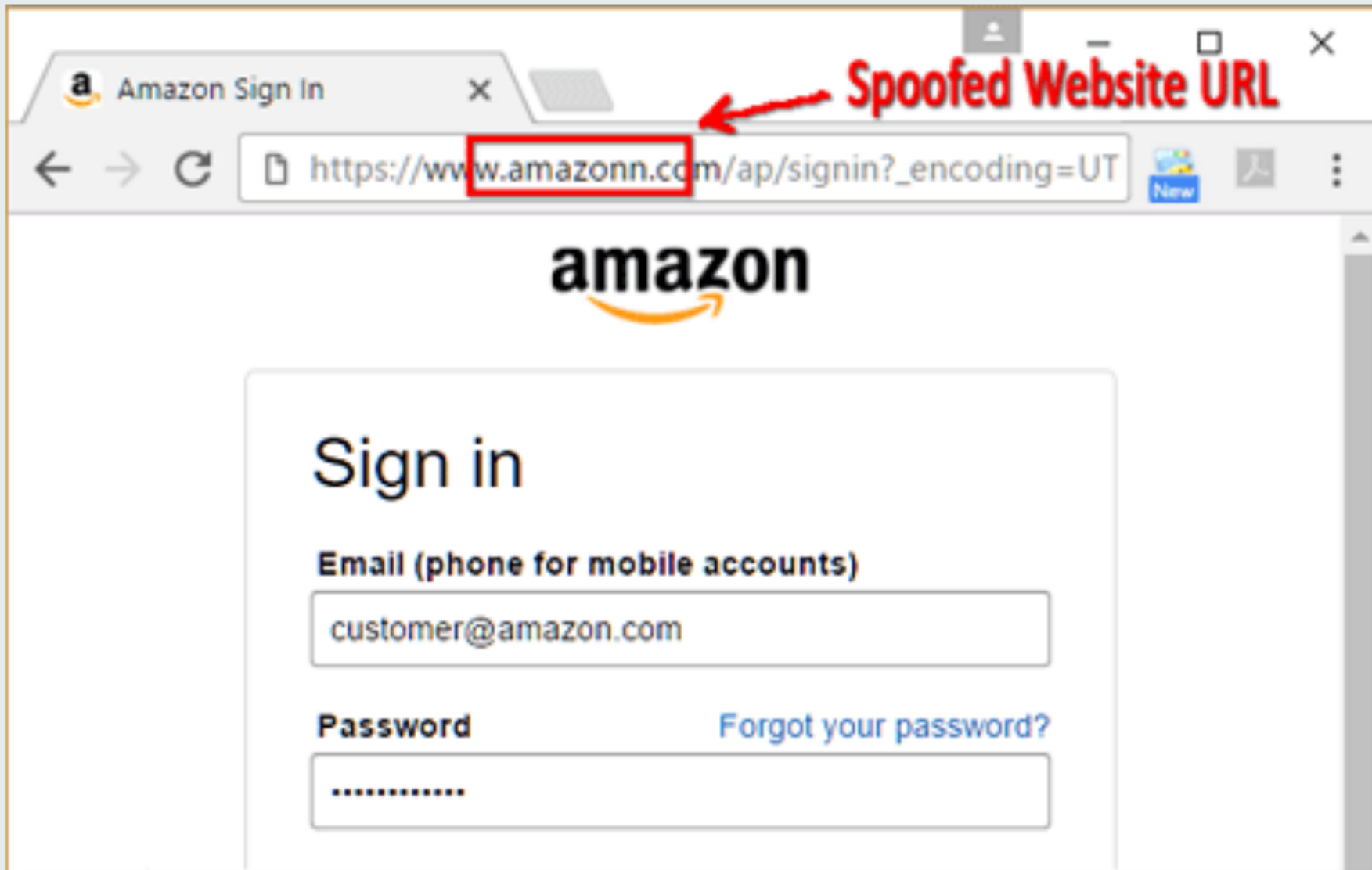
If you do not contact us, certain limitations may be placed on your debit card.

Grammatical Error

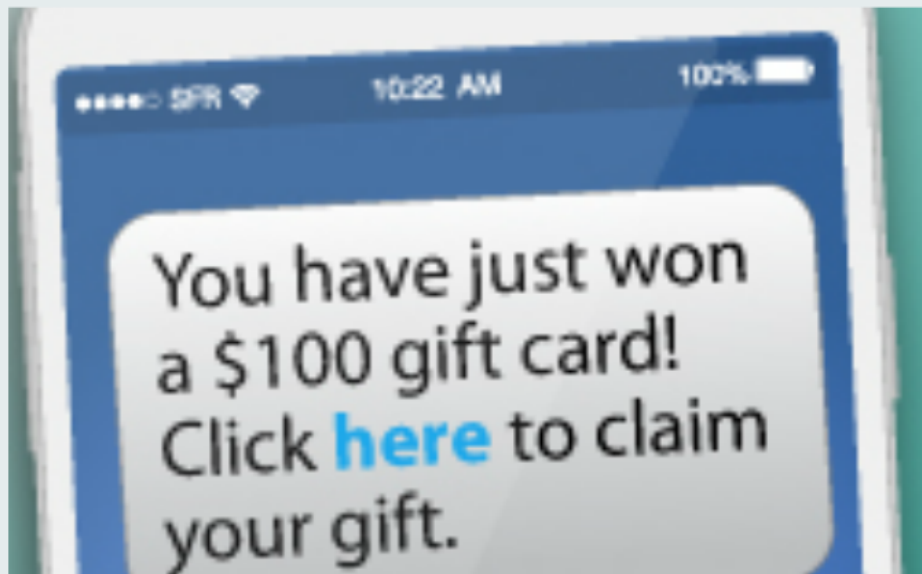
<http://bit.do/ghsdfhgds>

© 2014 Bank of America Corporation. All rights reserved.

Website Phishing



SMS Phishing (Smishing)



Text Message
Today 08:58

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



Voice Phishing (Vishing)



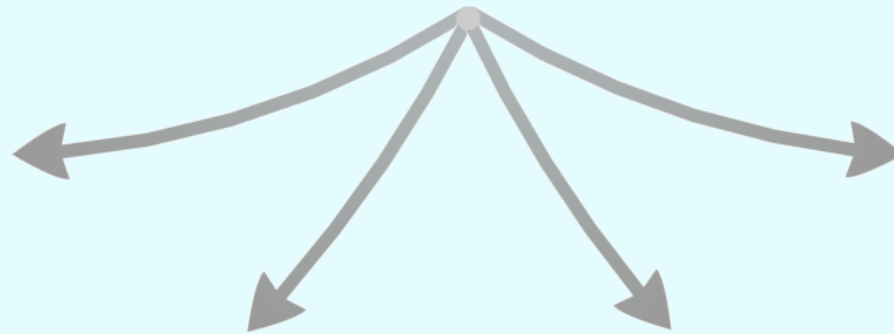
Virtual Fishing (Virtual)



Threat

Environmental

5%



Hardware

- Loss
- Damage
- Power Failure
- Malicious Hardware

Software

- Malicious software
 - Malware
- Hacking
 - Common Hacking Techniques

Human

- Insider Threat
- Social Engineering

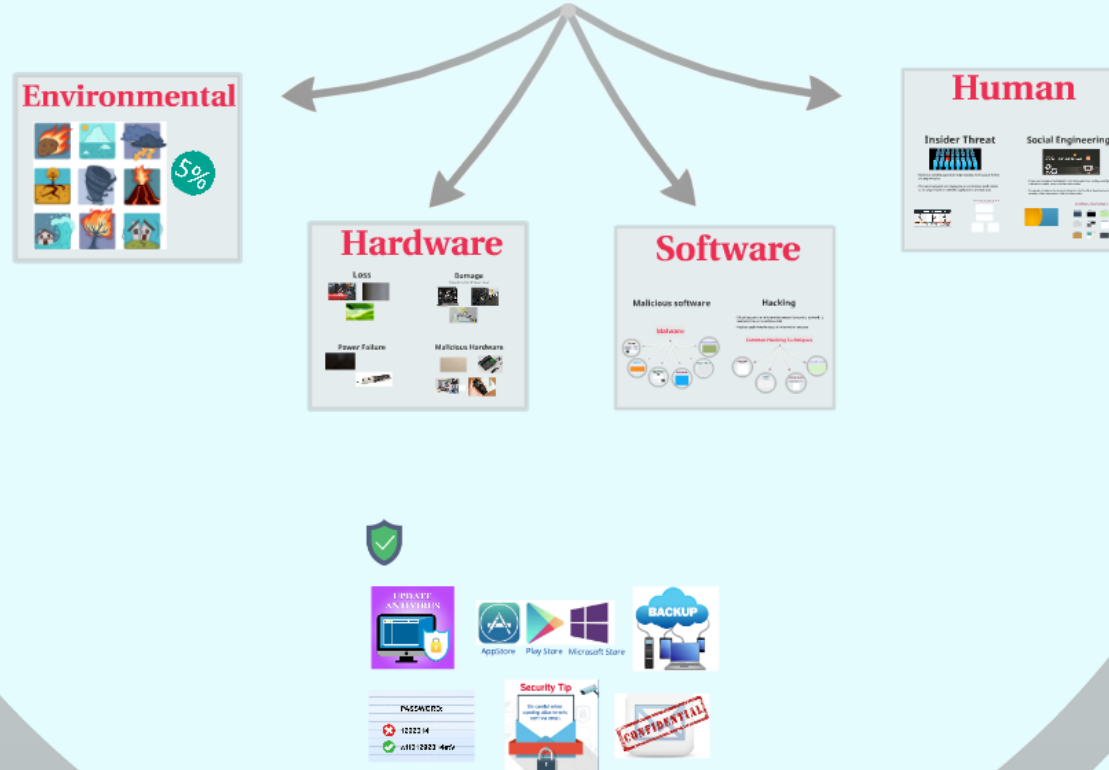




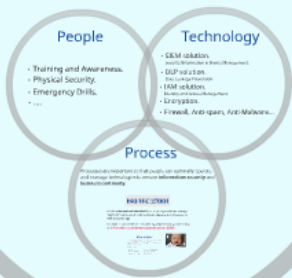
AppStore Play Store Microsoft Store



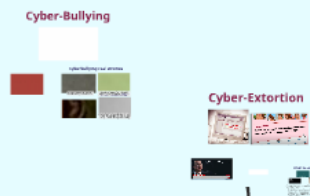
Threat



Countermeasures



CyberCrime



Information Security



Agenda

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

Thank You



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?

ISMS is a set of processes, policies, and procedures that are designed to protect an organization's information assets from unauthorized access, disclosure, alteration, and destruction.



It is a framework of controls that are designed to protect an organization's information assets from unauthorized access, disclosure, alteration, and destruction.

People

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

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

Process

Technology

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

ess.

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)**.

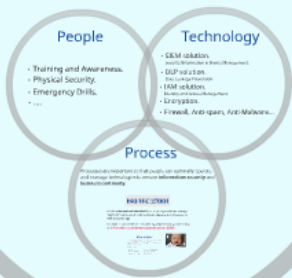
What is ISMS?

ISMS is a set of processes, policies, and procedures that are designed to protect an organization's information assets from unauthorized access, disclosure, alteration, and destruction.

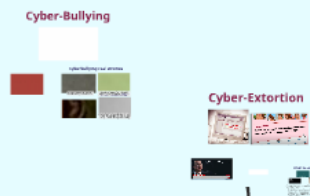


ISMS is a set of processes, policies, and procedures that are designed to protect an organization's information assets from unauthorized access, disclosure, alteration, and destruction.

Countermeasures



CyberCrime



Information Security



Agenda

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

Thank You



Preface



CyberCrime

Cyber-Bullying



Cyberbullying real stories



Cyber-Extortion



What to do?

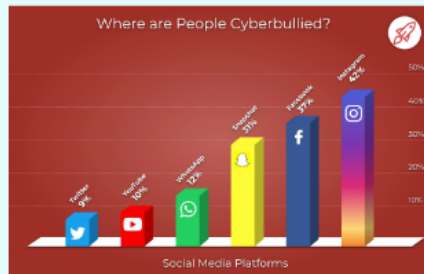
What to do?

It is important to report any cyberbullying or cyber extortion to the appropriate authorities. You should also take steps to protect your personal information and privacy. If you are a victim of cyberbullying or cyber extortion, you should seek support from friends and family. You should also consider seeking legal advice.

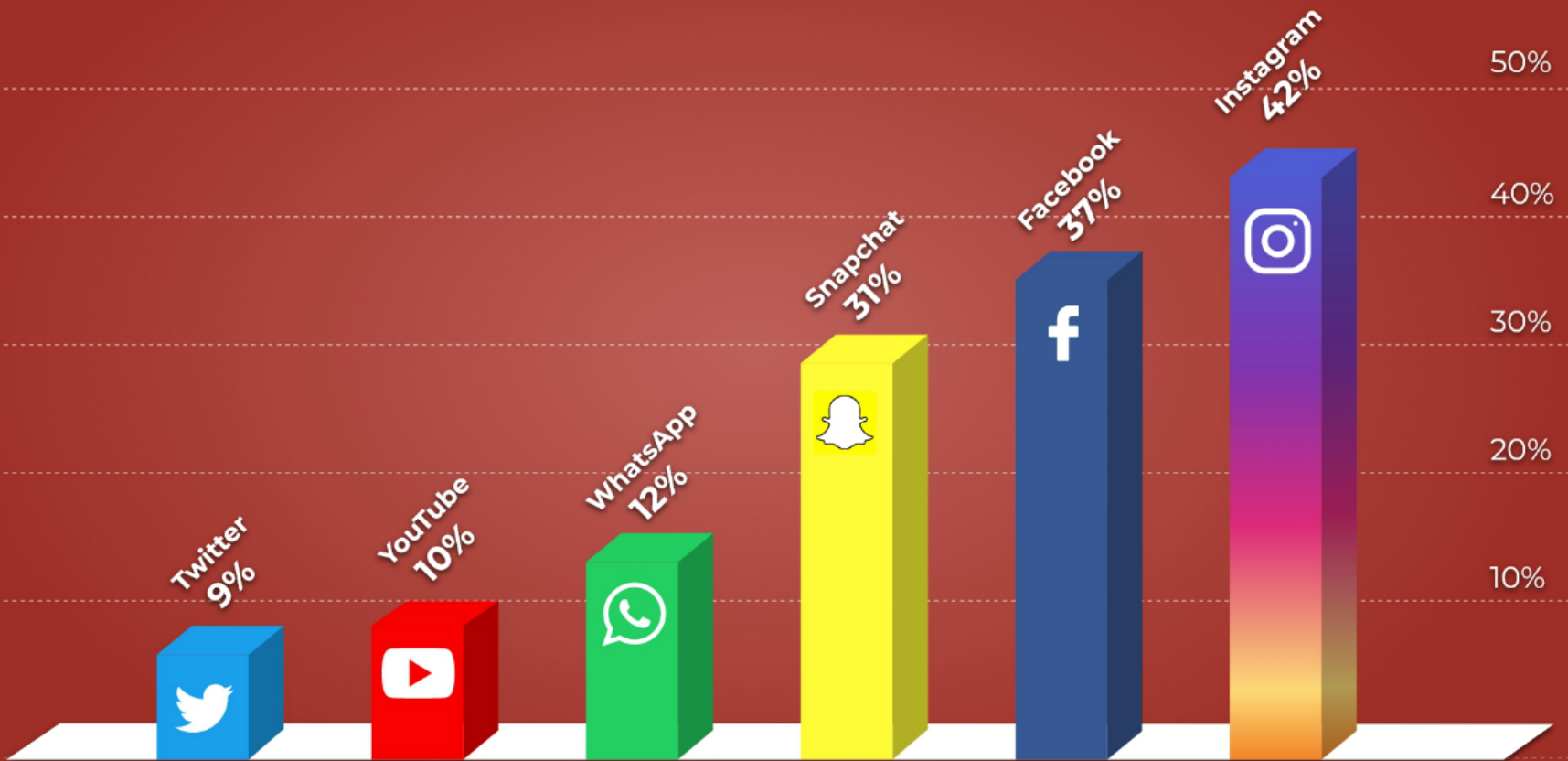
Cyber-Bullying



Cyberbullying real stories

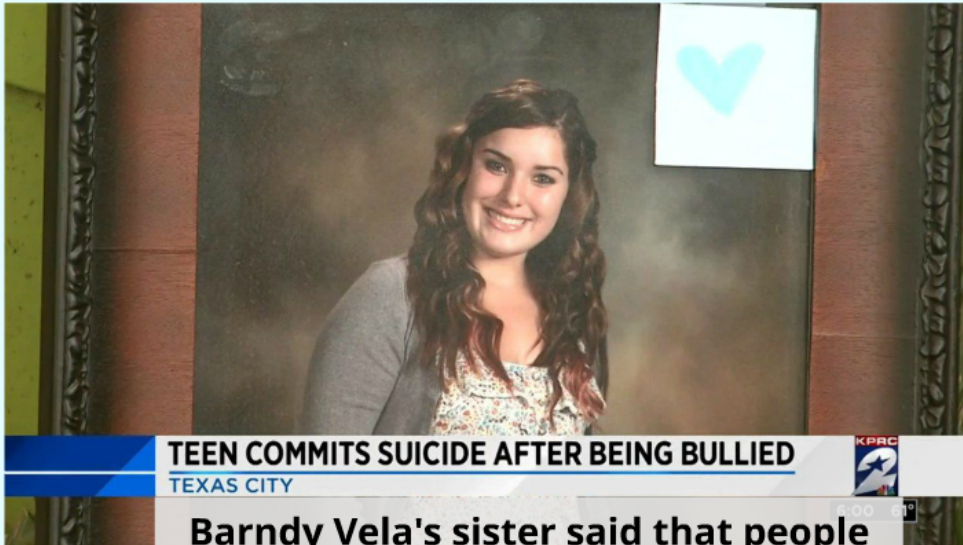


Where are People Cyberbullied?



Social Media Platforms

Cyberbullying real stories



TEEN COMMITS SUICIDE AFTER BEING BULLIED
TEXAS CITY

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

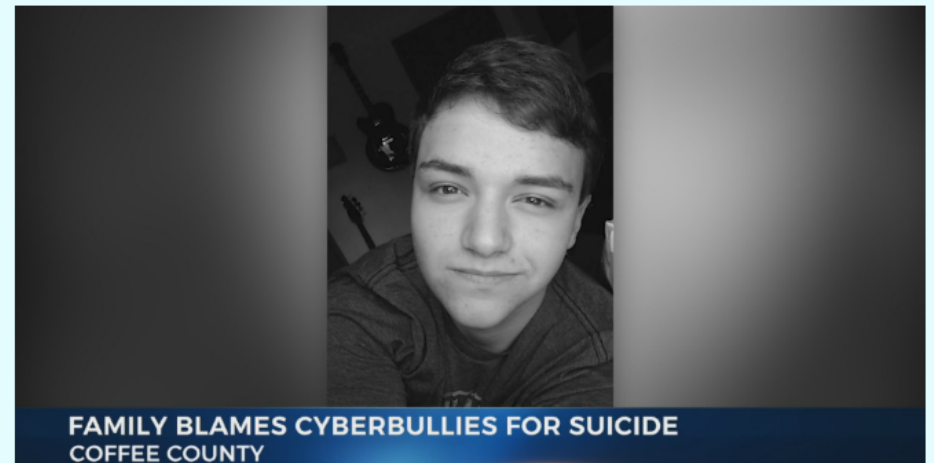


GIRLS SUSPECTED OF CYBER-BULLYING TEEN
Police: Rebecca Sedwick killed herself after being bullied

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



K-POP CYBERBULLYING
MALICIOUS ONLINE COMMENTS
CAN BE SIMILAR TO MURDER



FAMILY BLAMES CYBERBULLIES FOR SUICIDE
COFFEE COUNTY

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 stories



Cyber-Extortion

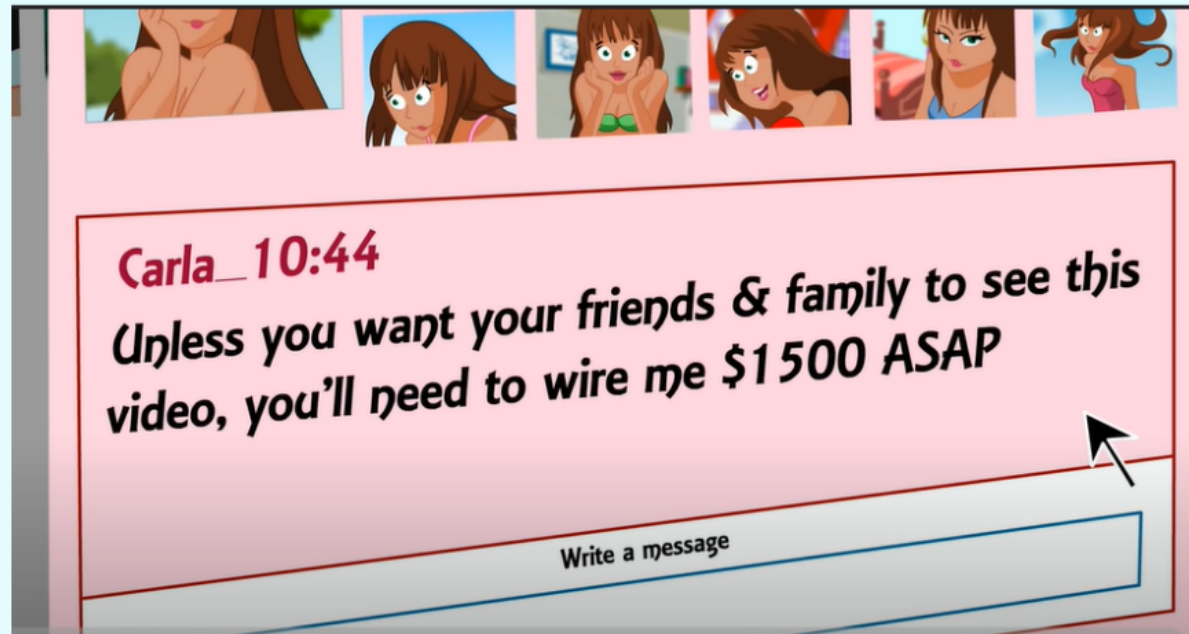
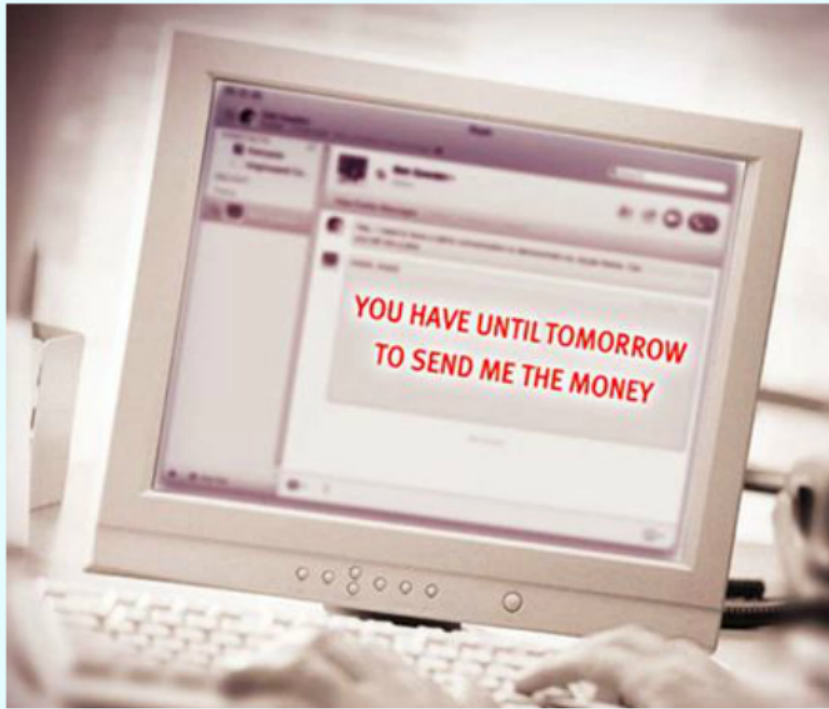


What to do?

What to do?

It's important to report cyberbullying and cyber extortion to the appropriate authorities. You should also take steps to protect your personal information and privacy. If you are being cyberbullied or extorted, you should stop using the internet and contact your local law enforcement agency.

Cyber-Extortion





"...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

CNN

4:26 PM PT



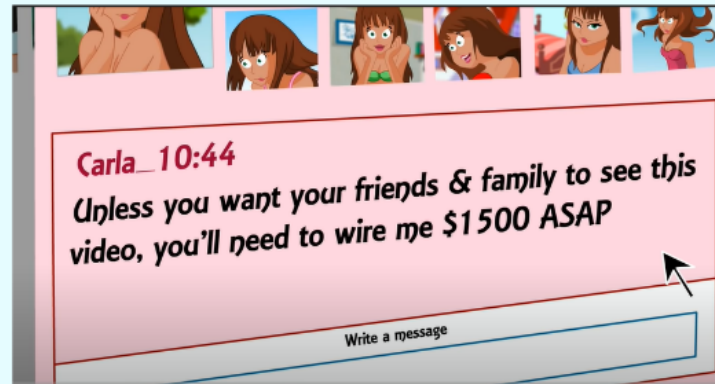
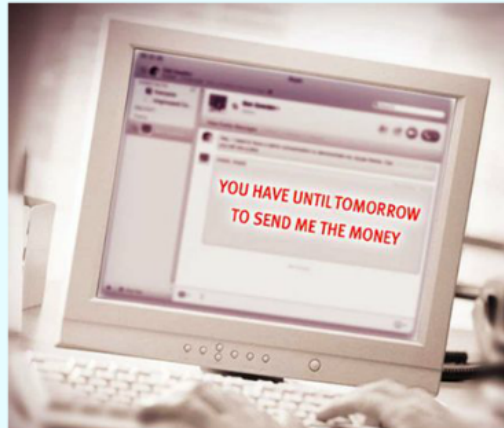
November 1 at 3:37 PM · 🌐

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

Cyber-Extortion



What to do?



- 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 your 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 التشريحي 17 لعام 2012

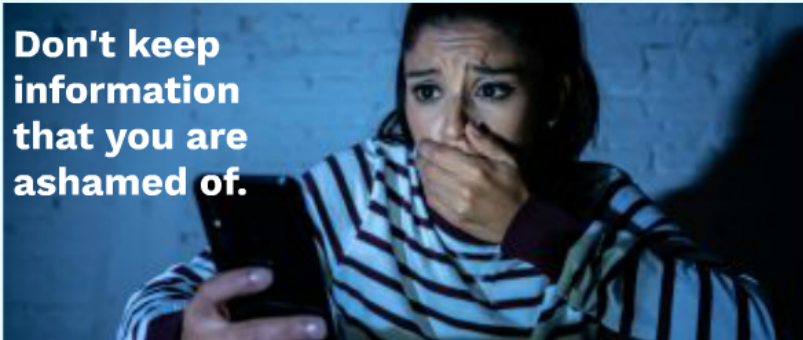
انهك حرية الحياة الخاصة ..
 يتلقى بالخبس من شهر إلى سنة أشهر والغرامة من مئة ألف إلى مئسة الف ليرة سورية كل من نشر
 عن طريق الشبكة معلومات تهتك خصوصية أي شخص دون رضاه حتى وإن كانت تلك المعلومات صحيحة .

What to do?



- **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.**

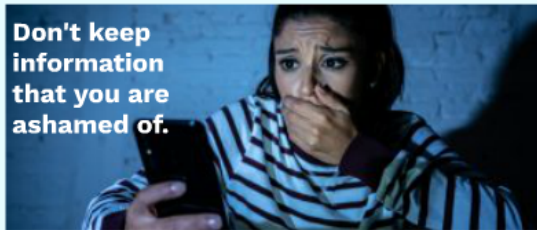
What to do?



someone threatens to share explicit images of you unless they pay them money:



What to do?



- **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.**

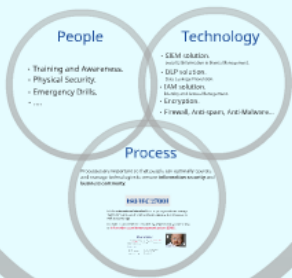
قانون التواصل على الشبكة ومكافحة الجريمة المعلوماتية

المادة 23 - المرسوم التشريعي 17 لعام 2012

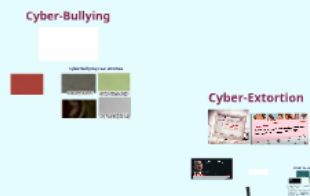
انتهاك حرمة الحياة الخاصة ..

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 شخص دون رضاه حتى ولو كانت تلك المعلومات صحيحة .

Countermeasures



CyberCrime



Information Security



Agenda

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

Thank You



Preface



Thank You

