QUIZ KEY:

August 23 2018

Introduction to Information Security & Privacy

* Protecting Assets
* Access
* Physical Hardware
* Data Integrity
* Can I access my Assets or not
* Confidentiality

Information Security

* Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction. The terms information security, computer security and information assurance are frequently used interchangeably.
* Protecting the confidentiality, integrity and availability of information and valuable assets.
* Information security is concerned with the confidentiality, integrity and availability of data regardless of the form the data may take: electronic, print, or other forms.

Privacy

* The relationship between the collection and dissemination of data.
* Privacy is a sensitive issue that we all concerned about to some degree. Nobody wants to think that his or her every move is being watched…on the computer or not! This is also true for electronic messaging, files, and email in the workplace. When these issues are raised, inevitably there are questions that follow.
* Who owns these electronic files?
* Who can access and disclose their data?

Information Security Facts

* United States
  + 2013: $11.56
  + 2014: $12.69
  + 2015: $15.42
* Germany
  + 2013: $7.56
  + 2014: $8.13
  + 2015: $7.50
* Japan
  + 2013: $6.73
  + 2014: $6.91
  + 2015: $6.81
* United Kingdom
  + 2013: $4.72
  + 2014: $5.93
  + 2015: $

Cybersecurity Threats

* Ransomware- Holding organizations data for ransom has surged up in recent times at a phenomenal rate. And SonicWall reports that ransomware attempts have swelled up from 2.8 million in 2015 to 638 million last year. Intel Security 2017 report also confirms that as much as $209 million was paid in 1Q of 2016 alone. Thus, the amount paid says a lot about malware developers who are using this malicious software to earn their living.
* Internet of Things Botnets- In late 2016, when en enormous DDoS attack was launched on DNS Service Provider called DYN, the attack proved that many service providers were ill-equipped to deal with the scope of the latest cyber attacks. Mirai Botnet was found to be the culprit and this instance shocked the entire business community which otherwise thought that security in IoT devices was just secondary. So, IoT.
* Phishing and Whaling attacks- ‘Phishing’ is a concept where hackers send fraudulent emails from trusted accounts to target businesses through individual staff members. When an innocent staff member clicks on the email, then attachment which is tagged to the email starts functioning releasing a malware capable of stealing data. ‘Whaling’ takes the above said cyber attack strategy to next level by targeting high worth individuals, often CIOs or CEOs of a firm. FBI has warned all corporates operating in and out of United States about this scam and confirmed that hackers have succeeded in making $3 million from such fraudulent transactions last year.
* Business Process Compromise Attacks- Trend Micro has described this concept of cyber attack as a relatively new phenomenon where hackers are using techniques to manipulate the day to day operations of a business in their favor. For instance, in the year 2013 drug traffickers from South America managed to intercept the network of an Antwerp to track the movement and location of containers. This helped the traffickers to re.
* Machine Learning enabled attacks- It looks like the technology of Artificial Intelligence seems to be serving both the good and bad people.

Cyber attacks directed at social media.

* Like-jacking: occurs when criminals post fake Facebook “like” buttons to webpages. Users who click the button don’t “like” the page, but instead download malware.
* Link-jacking: this is a practice used to redirect one website’s links to another which hackers use to redirect users from trusted websites to malware infected websites that hide drive-by downloads or other types of infections.
* Phishing: the attempt to acquire sensitive information such as usernames, passwords, and .

Changing Attacker Profiles

* Recreational
  + Fame and notoriety
  + Limited technical resources
  + Known exploits
* Criminal
  + Vandalism
  + Limited technical capabilities
* Hacktivist
  + Statement
  + Relentless, emotionally committed
  + Vast networks
  + Targeted attacks
* Organized Crime
  + Economic gain
  + Significant technical resources and capabilities
  + Established syndicates
  + Adware, crimeware, IP theft
* State Sponsored
  + Cyberwar, state secrets, industrial espionage
  + Highly sophisticated
  + Nearly unlimited resources
  + Advanced persistent threats

What can you do to get protected:

* Don’t click any strange links
* Educate yourself about how cyber attacks look and work on social media platforms and learn how to protect your Facebook, LinkedIn, Twitter and Instagram accounts.
* Install a solution that can protect you against malware and dangerous web locations.

Security Incidents & Breaches

* Over 70% of organizations report having been compromised by a successful cyberattack.
* 71% were affected by a successful cyberattack in 2014, but only 52% expect to fall victim again in 2015.
* Security incidents grew 66% CAGR.
* 21%