Cysec Assignment-2

S.SriNithya
19261A04B5
3-ECE-2

1. Explain various security challenges posed by mobile devices?

• Mobility brings two main challenges to cybersecurity

i, first, on the hand-held devices, information is being taken outside the physically controlled environment and.

ii, second remote access back to the protected environment is being granted.

• Perceptions of the organizations to these cybersecurity challenges are important in devising appropriate security operating procedure

• As the number of mobile device user increases, two challenges are presented :

* at the device level called "micro challenges" and

* at the organization level called "macro challenges".

• Some well-known technical challenges in mobility security are; managing the registry settings and configurations, crypotography security, remote access server (RAS) security, networking application program interface (API) security etc.

2. Define insider threat? Explain any 2 insider threats with a neat diagram.

Insider threat :- It is defined as "the misuse or destructio of sensitive or confidential information, as well as IT equipment that houses this data by employees, contractors, and other 'trusted' individuals.

i, Heartland payment system fraud :

• A case in point is the infamous "Heartland payment system fr that was uncovered in January 2010. This incident brings out glaring point about seriousness "of insider attack".

• In this case, the concerned organization suffered a serious bl through early 100 million credit cards compromised from a

- In this case a piece of malicious software planted on a company's payment processing network. to Heartland by Payment card data as it was being sent for process to Heartland by thousand's of companies retails clients.

- Digital information within the magnetic stripe on the back of credit and debit cards was copied by Keylogger.

ii Blue shield Blue cross (BCBS) :-

- Yet another incidence is the BCBS data breach in october 2009- the theft of 57 hard drives from a Bluecross Blueshield of tennessee training faculty puts the private information of approximately 500,000 customers at risk in atleast 32 states.

- Three hard drives contains (3.5 x 10) were physically removed from server racks on computer inside data storage closer at a training center.

- The two lessons to be learn't from this are

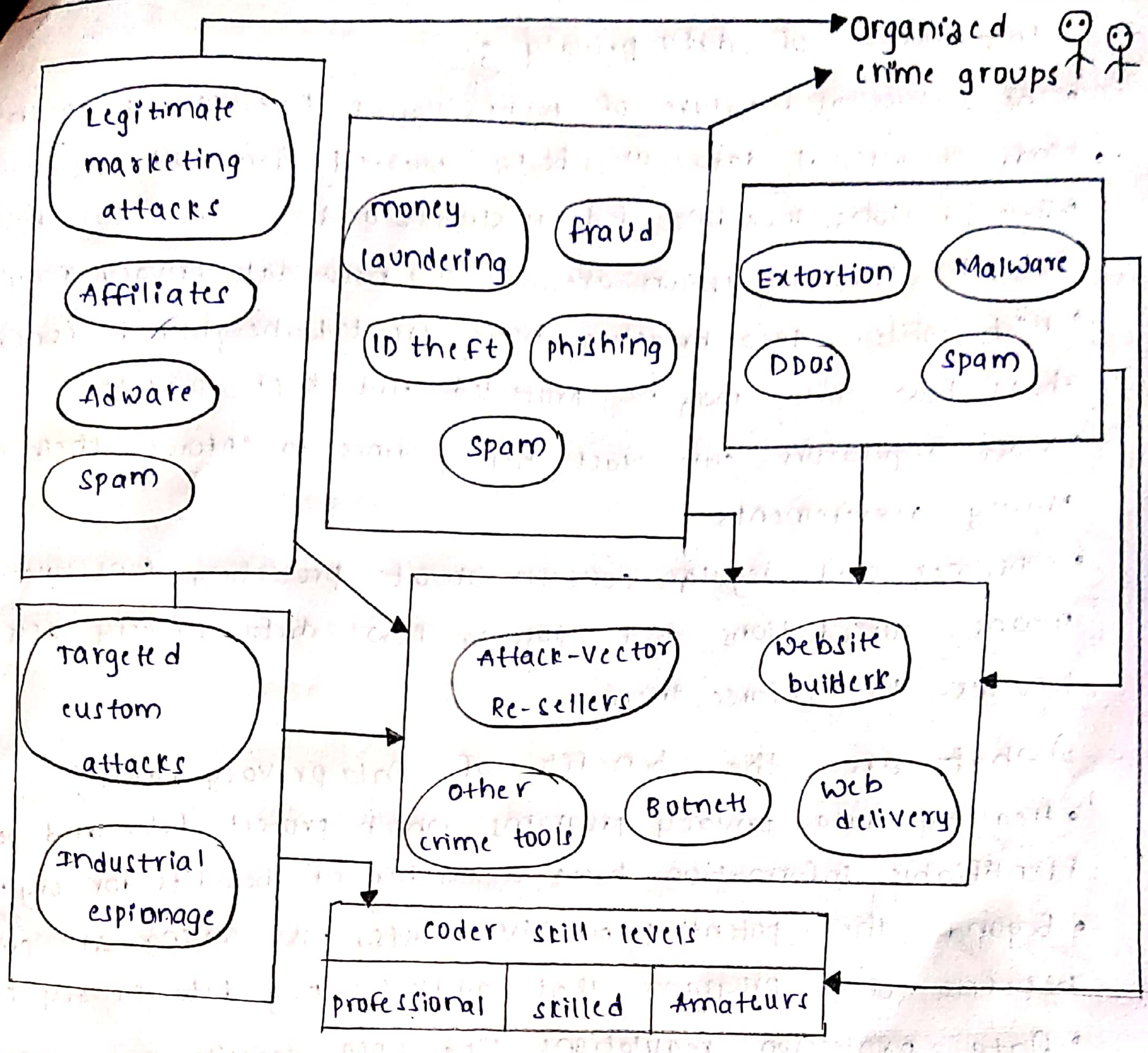
* physical security is very important.

* insider threats cannot be ignored.

- what makes matters worse is that the groups/agencies/ entities. connected with cyber crimes are all linked.

Eg is shown below

[P.T.O]



cybercrime - the flow and connections

a) what is data privacy ? why it is important ?

Data privacy :- Data privacy or infomation privacy is concerned with proper handling ,processing, storage and usage of personal information. It is all about the rights of individuals with respect of their personal information

most common concerns regarding data privacy are :-

- managing contracts or policies.
- applying governing regulation or law
- Third-party management.

Importance of data privacy :-

- The sophisticated nature of technological development means ne kinds of personal data are being collected from customers & citizen
- Jurisdictions including federal, states, and international bodies like the European Union are enacting new data privacy regulation
- High-profile data breaches have created heightened concern about how data may be protected and kept private.
- Most regulators can exact hefty fines to enforce their data privacy requirements.
- consumer and regular concern about protecting sensitive data means jurisdictions and passing new data privacy acts and Penalties to enforce them.

b) what are the benefits of Data privacy Laws?

- Healthy data privacy programs which protect data and personali identifiable information have a number of benefits for organizatio
- Beyond the potential punitive costs, cost-savings are possible benefits of a program that addresses key data privacy issues.
- Data protection regulations like GDPR require not only Safeguarding user data, but also responding and sharing data upon request.
- clean, efficient processes for the organization to meet these data governance obligations can reap substantial cost-savings.
- An organization that demonstates a solid understanding of data privacy principles is often seen as a leader in their category.

riefly explain the following

a) IP spoofing :-

spoofing is an impersonation of a user, device or client on the internet. It's often used during a cyberattack to disguise the source of attack traffic. The most common forms of spoofing are : DNS server spoofing - modifies a DNS server in order to redirect a domain name to a different IP address.

b) smishing :-

- smishing is a criminal offense conducted by using social engineering techniques similar to phishing.
- This name is derived from "SMS phishing."
- SMS can be abused by using different methods and techniques other than information gathering under cybercrime.
- smishing uses cell phone text messages to deliver a lure message to get the victim to reveal his|her PI.
- smishing works in the similar pattern as vishing.

c) vishing :-

- vishing is the criminal practice of using social engineering over the telephone system, most often using features facilitated by VOIP, to gain access to personal and financial information from the public for the purpose of financial reward.
- The term is a combination of V-voice and phishing.
- vishing is usually used to steal creditcard numbers or order related data used in ID theft schemes from individuals.
- most profitable uses of the information gained through vishing attack include :

* ID theft
* transfering money funds
* monitoring the victims bank accounts.

write short notes on email spoofing discuss about Hacking happened to official Twitter Account of Modi.

Email spoofing is a form of cyber attack in which a hacker sends an email that has been manipulated to seem as if is originated from a trusted source. Email spoofing is a popular tactic used in phishing and spam campaigns because people are more likely to open an email when they think it has been sent by a known sender.

Hacking happened to official Twitter account of Modi:

The twitter handle of PM @narendr Modi was very briefly compromised. The matter was escalated to twitter and the account has been immediately secured. In the brief peri that the account was compromised, any tweet shared mus be ignored," PMO india said in a tweet".

Before the account was restored, a tweet was shared with a URL on PM modi's timeline which read, "India has officially adopted bitcoin as legal tender. The government h officially bought 500 BTC and is distributing them to all residents of the country.

According to sources, the ministry of Electronics and Information Technology's indian computer Emergency Response Team (CERT-IN) is on the job and is trying to identify the source of the hacking incident. Latest technology is being used for the same.

—x—