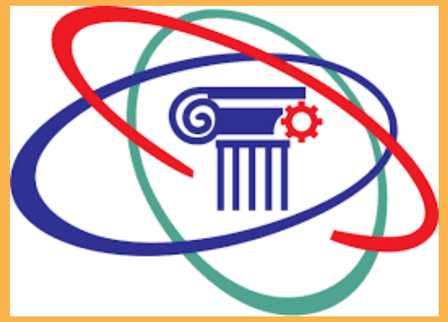
ACROPOLIS INSTITUTE OF TECHNOLOGY AND RESEARCH



SUBJECT: EVALUATION OF INTERNSHIP

TOPIC :- Classifications of Cybercrimes

SESSION : 2022-23

SUBMITTED BY:

Jitendra Aakde

(0827CI201088)

SUBMITTED TO:

PROF. NIDHI NIGAM

CONTENT

- E-Mail Spoofing
- Spamming
- Internet Time Theft
- Salami attack
- Salami Technique

E-Mail Spoofing

Email spoofing is a technique used in spam and phishing attacks to trick users into thinking a message came from a person or entity they either know or can trust. In spoofing attacks, the sender forges email headers so that client software displays the fraudulent sender address, which most users take at face value. Unless they inspect the header more closely, users see the forged sender in a message. If it’s a name they recognize, they’re more likely to trust it. So they’ll click malicious links, open malware attachments, send sensitive data and even wire corporate funds.

Email spoofing is possible due to the way email systems are designed. Outgoing messages are assigned a sender address by the client application; outgoing email servers have no way to tell whether the sender address is legitimate or spoofed.

Recipient servers and antimalware software can help detect and filter spoofed messages. Unfortunately, not every email service has security protocols in place. Still, users can review email headers packaged with every message to determine whether the sender address is forged.

Spamming

Spam is any kind of unwanted, unsolicited digital communication that gets sent out in bulk. Often spam is sent via email, but it can also be distributed via text messages, phone calls, or social media.

What does spam stand for?

Spam is not an acronym for a computer threat, although some have been proposed (stupid pointless annoying malware, for instance). The inspiration for using the term “spam” to describe mass unwanted messages is a Monty Python skit in which the actors declare that everyone must eat the food Spam, whether they want it or not. Similarly, everyone with an email address must unfortunately be bothered by spam messages, whether we like it or not.

If you’re interested in the origins of spam in greater detail, see the history of spam section below.

Internet Time Thefts

Hacking the username and password of ISP of an individual and surfing the internet at his cost is Internet Time Theft.

As one of the most common forms of time theft, this is when employees use the internet for non-work purposes. They could be using it for browsing the internet, online shopping, playing games, or spending bulks of time on social media.

Salami Attack

It is an attack which proceeds with small increments and final add up to lead to a major attack. The increments are so small that they remain unnoticed. An example of salami attack is gaining access to online banking of an individual and withdrawing amount in such a small amounts that it remains unnoticed by the owner. Often there is default trigger set in the banking website and transactions below say, Rs. 1000 withdrawal are not reported to the owner of the account. Withdrawing amount of Rs. 1000 over a period of time will lead to total withdrawal of a large sum.

salami technique

How does a salami attack work?

After attempting many different routing and bank account mixtures to gain access to accounts, cybercriminals can make negligible deposits into users' accounts once they find a valid account. They can set up small monthly fees to be withdrawn from the financial institution and placed into accounts they can access once they find an account.

The idea is that because the fees are so minor, users will ignore them on their bank statements. However, if hackers successfully deploy this illegal strategy throughout other hundreds of bank accounts, their earnings can rapidly increase.