PHISHING AND
ANTIPHISHING

Shireesha.B (08315A0505)
Contents:

- Introduction
- Phishing
- Phishing Techniques
- Anti-Phishing
- Anti-Phishing Techniques
- Conclusion
What is Phishing?:

- Phishing, a term coined in 1996, is a form of online identity theft.
- Pronounced "fishing".
- Scam to steal confidential information such as credit cards, social security numbers, user IDs and passwords.
Steps in phishing attack:

1. The phisher sends an email to the victim.
2. The victim views the email.
3. The victim clicks on a link in the email that leads to a phishing website.
4. The phisher receives the victim's information.
5. The victim enters their login credentials on the phishing website.
Phishing Techniques:

- Phishing through email and spam
- Phishing using key loggers.
- Phone phishing
- Tab nabbing
Email and spam:
Phishing through key-loggers:

- A key logger is something that records key strokes made on the computer.
- It captures every key pressed on the keyboard and stores it down a file or memory bank that can be viewed by the person performing the monitoring in real time or a later date.
- There are two types of key loggers:
  - Hardware keyloggers
  - Software keyloggers.
- Hardware-keylogger

- Software-keylogger:
Phone phishing:

- Messages that claimed to be from a bank told users to dial a phone number regarding problems with their bank accounts.

- Once the phone number was dialed, prompts told users to enter their account numbers and PIN, where details are hacked.
Tabnabbing

- Of the multiple tabs that users use and silently redirects a user to the affected site.
A NEW TYPE OF PHISHING ATTACK

The web is a generative and wild place. Sometimes I think I missed my calling; being devious is so much fun. Too bad my parents brought me up with scruples.

Most phishing attacks depend on an original deception. If you detect that you are at the wrong URL, or that something is amiss on a page, the chase is up. You’ve escaped the attackers. In fact, the time that wary people are most wary is exactly when they first navigate to a site.

What we don’t expect is that a page we’ve been looking at will change behind our backs, when we aren’t looking. That’ll catch us by surprise.

HOW THE ATTACK WORDS

1. A user navigates to your normally looking site.
WHY PHISHING ATTACK!

- Lack of Knowledge
  - computer system
  - security and security indicators
  - web fraud

- Visual Deception
  - Visually deceptive text
Lack of knowledge of security and security indicators
Lack of knowledge of web-fraud

Spoofed Page and Address Bar

Not the real address bar
Visually Deceptive Text

Original website

Phishing website
Anti-Phishing:

- Anti-phishing techniques are used to prevent and detect phishing attacks.
Anti-phishing techniques:

- Social Responses
- Filter evasion
- One time passwords
Social Responses:

- One strategy to overcome phishing is to train people to recognize phishing attempts, and to deal with them.
- This is done by educating a user.
- PhishGuru teaches people how to protect themselves from phishing attacks.
Filter Evasion:

- Here, images are used instead of CAPTCHAs to make it harder for phishers. (A image with several option)
One Time Passwords

- A one-time password (OTP) is a password that is valid for only one login session or transaction.
- OTPs avoid a number of shortcomings that are associated with traditional (static) passwords.
- The most important shortcoming that is addressed by OTPs is that, in contrast to static passwords, they are not vulnerable to replay attacks.
Techniques of implementing One Time Passsswords

- Key sending one time password to mobile:

  Generated dynamically for a period of time.
• **Key chain:**
  Dynamic passwords are sent to key chain. A small hardware device in which the one time password will be displayed for any given amount of time.
Software tools option:

A software will be installed in the user system/device, by which the user can have OTP and which will be updated for certain amount of time.
• Web Based Method:

Identify your categories and enter the characters below.

Access Code: [ ] [ ] Submit
Conclusion:

- Phishing is an important problem that results in identity theft. Although simple, phishing attacks are highly effective and have caused billions of dollars of damage in the last couple of years.
- By implementing the anti-phishing techniques, we overcome all the security problems and thus information can be confidential.
QUERIES?