CONTENTS

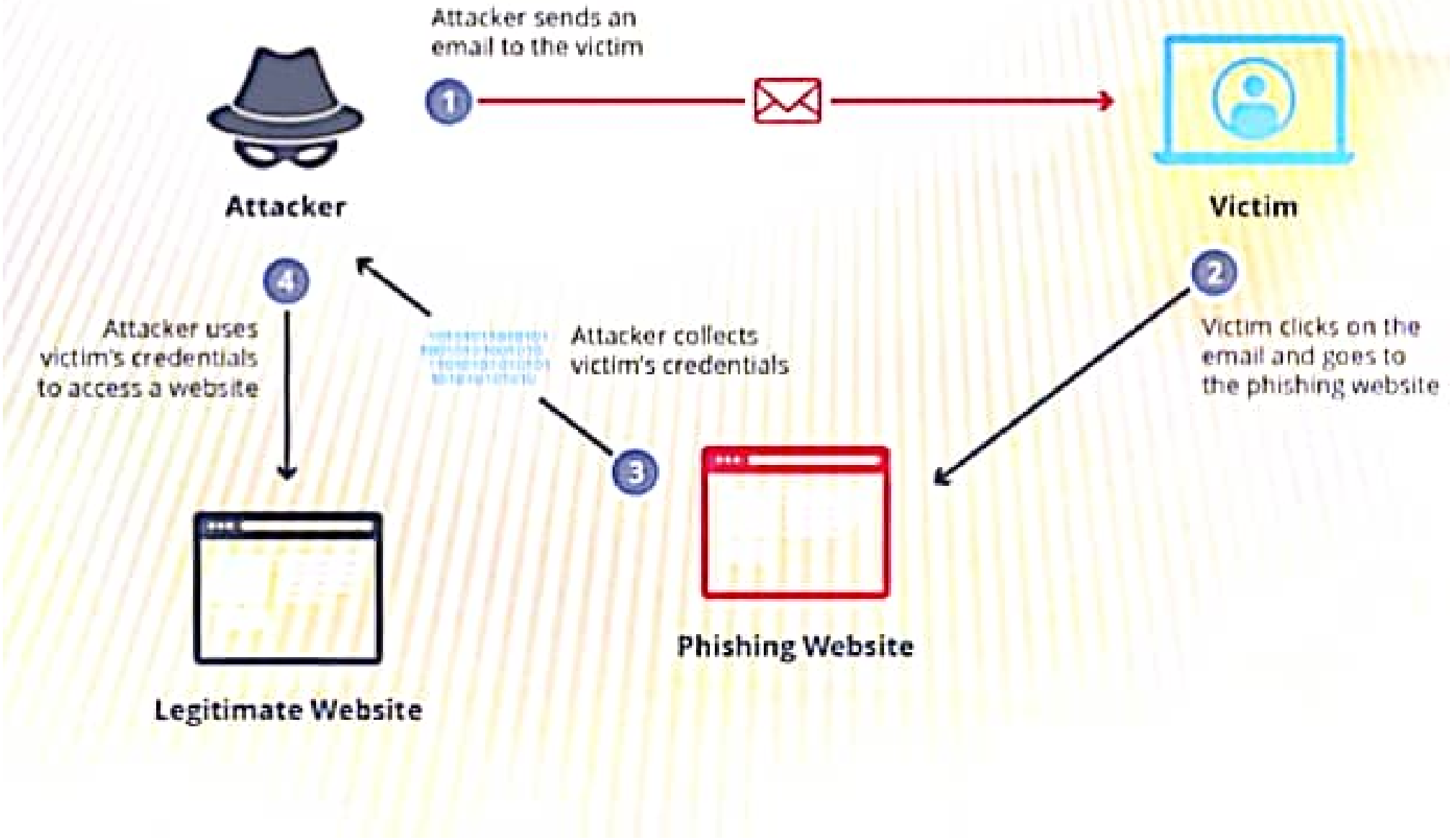
INTRODUCTION

- Phishing is the most powerful and popular attack for hacking into emails and web accounts.
- Cyber criminals use this attack to hack into bank accounts, Facebook accounts and email account of innocent people.
- Every year, most of the biggest cyber crime case involve this attack.
- So we must know what is Phishing and how to protect your accounts from phishing attack.

WHAT IS PHISHING?

- Phishing is the act of fooling a computer user into submitting personal information by creating a counterfeit it website that looks like a real (and trusted)site.
- It is a hacker technique of "fishing" for passwords and other secret financial info.

HOW DOES PHISHING WORK?



TYPES OF PHISHING:

1) Deceptive phishing
2) Spear phishing
3) Whaling
4) Pharming

TYPES OF PHISHING

1. **Deceptive phishing:**

- Sending a deceptive email, in bulk, with a "call to action" that demands the recipient click on a link.
- In this case, an attacker attempts to obtain confidential information from the victims.
- Attackers use the information to steal money or to launch other attacks.
- E.g A fake email from a bank asking you to click a link and verify your account details.

TYPES OF PHISHING

2. Spear phishing:

- Spear phishing targets specific individuals instead of a wide group of people.
- Attackers often research their victims on social media and other sites.
- That way, they can customize their communications and appear more authentic.
- Spear phishing is often the first step used to penetrate a company's defenses and carry out a targeted attack.

TYPES OF PHISHING

3.Whaling:

- When attackers go after a "big fish" like a CEO, it's called whaling.
- These attackers often spend considerable time profiling the target to find the opportune moment and means of stealing login credentials.
- Whaling is of particular concern because high-level executives are able to access a great deal of company information.

TYPES OF PHISHING

4.Pharming

- Similar to phishing, pharming sends users to a fraudulent website that appears to be legitimate.
- However, in this case, victims do not even have to click a malicious link to be taken to the bogus site.
- Attackers can infect either the user's computer or the website's DNS server and redirect the user to a fake site even if the correct URL is typed in.

WHAT THE ARE DANGERS OF PHISHING ATTACKS?

- Sometimes attackers are satisfied with getting a victim's credit card information or other personal data for financial gain.
- Other times, phishing emails are sent to obtain employee login information or other details for use in an advanced attack against a specific company.

HOW DO I PROTECT AGAINST PHISHING ATTACKS?

1.User education

- One way to protect your organization from phishing is user education.
- Education should involve all employees.
- High-level executives are often a target Teach them how to recognize a phishing email and what to do when they receive one.
- Simulation exercises are also key for assessing how your employees react to a staged phishing attack.

2.Security technology

- No single cyber security technology can prevent phishing attacks.
- Instead, organizations must take a layered approach to reduce the number of attacks and lessen their impact when they do occur.
- Network security technologies that should be implemented include email and web security, malware protection, user behavior monitoring, and access control.

CAUSES OF PHISHING

- Misleading e-mails
- No check of source address
- Vulnerability in browsers
- No strong authentication at websites of banks and financial institutions
- Limited use of digital signatures
- Non-availability of secure desktop tools
- Lack of user awareness
- Vulnerability in applications

EFFECTS OF PHISHING

- Internet fraud
- Identity theft
- Financial loss to the original institutions
- Difficulties in Law Enforcement Investigations
- Erosion of Public Trust in the Internet.

CONCLUSION

- No single technology will completely stop phishing.
- However, a combination of good organization and practice, proper application of current technologies, and improvements in security technology has the potential to drastically reduce the prevalence of phishing and the losses suffered from it.