TCS332
Fundamental of Information Security and Blockchain

B. Tech CSE III Semester

Instructor:

Dr Mohammad Wazid

Professor, Department of CSE

Graphic Era (Deemed to be University), Dehradun, India

Email: wazidkec2005@gmail.com

Homepage: https://sites.google.com/site/mwazidiiith/home

Phishing attack

- Phishing is a cyber attack which involves social engineering often used to steal user data, including login credentials and credit card numbers.
- It occurs when an attacker, masquerading as a trusted entity, dupes a victim into opening an email, instant message, or text message.

Phishing attack

- The recipient is then tricked into clicking a malicious link, which can lead to the installation of malware, the freezing of the system as part of a ransomware attack or the revealing of sensitive information.
- This results in unauthorized purchases, the stealing of funds, or identify theft.

- Phishing is also used to gain a foothold in corporate or governmental networks as a part of a larger attack, such as an advanced persistent threat (APT) event.
- In that case, employees are compromised in order to bypass security perimeters, distribute malware inside a closed environment, or attacker can gain privileged access to the secure data.

- An organization suffered from such an attack typically sustains severe financial losses, declining of market share, reputation, and consumer trust.
- A business will have a difficult recovery time.

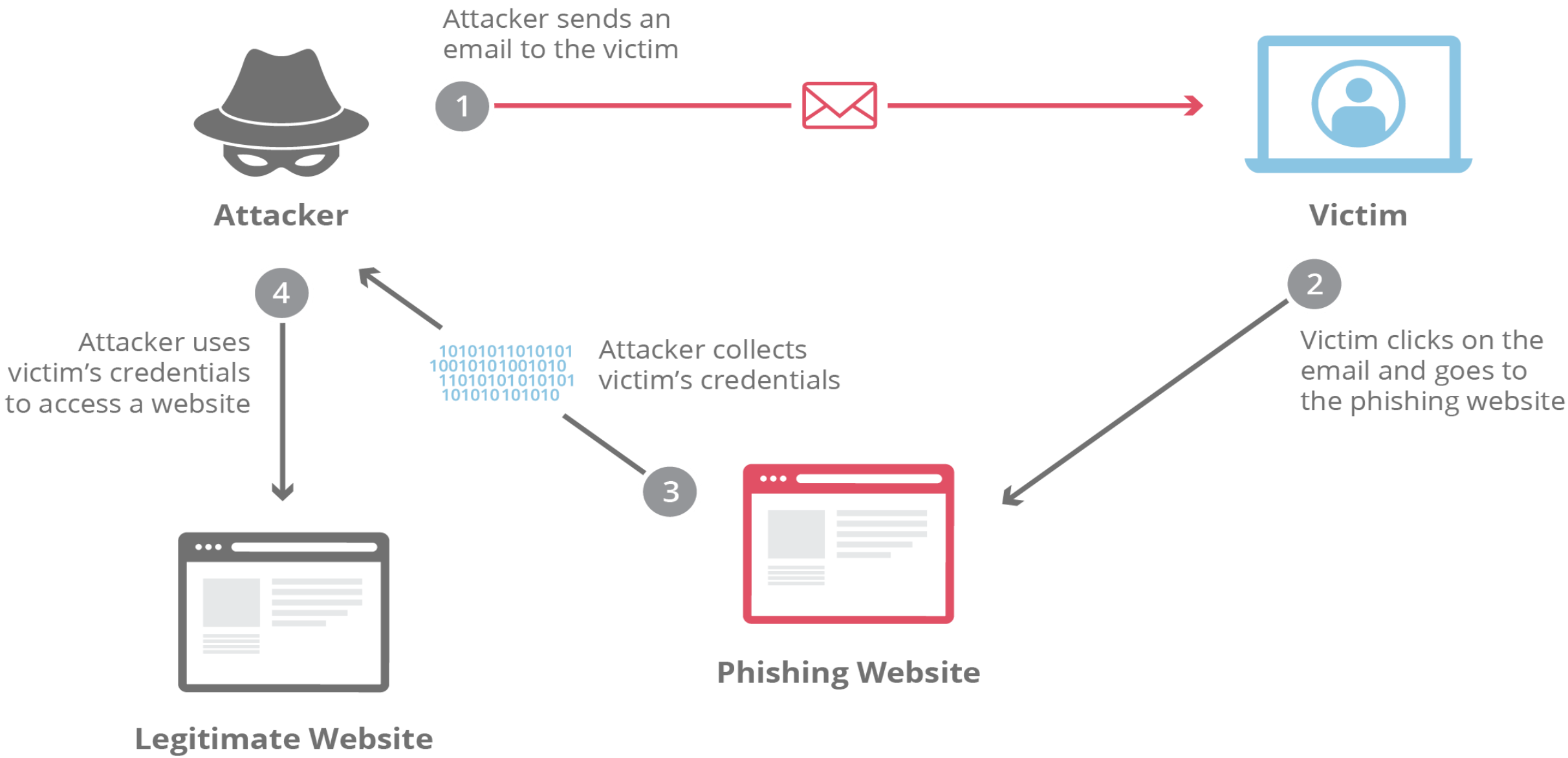

Fig. Phishing attack scenario
(source: https://www.cloudflare.com/learning/security/threats/phishing-attack/)

Phishing techniques

1. Email phishing scams

- Email phishing is a numbers game. An attacker sending out thousands of fraudulent messages. Even if only a small percentage of recipients fall for the scam.
- For this purpose attacker will go to create phishing messages to mimic actual emails from a spoofed organization.

Phishing techniques

1. Email phishing scams

- Using the same phrasing, typefaces, logos, and signatures makes the messages appear legitimate.
- In addition, attackers will usually try to push users into action by creating a sense of urgency.

1. Email phishing scams

- For example, an email could threaten account expiration and place the recipient on a timer.
- Applying such pressure causes the user to be less diligent and more prone to error.
- Lastly, links inside messages resemble their legitimate counterparts, but typically have a misspelled domain name or extra subdomains.

1. Email phishing scams

- For example, the **myuniversity.edu/renewal** URL was changed to **myuniversity.edurenewal.com.**
- Similarities between the two addresses offer the impression of a secure link, making the recipient less aware that an attack is taking place.

2. Spear phishing

- Spear phishing targets a specific person or enterprise, as opposed to random application users.
- It’s more in-depth version of phishing that requires special knowledge about an organization, including its power structure.
- A attacker researches names of employees within an organization’s marketing department and gains access to the latest project invoices.

2. Spear phishing

- Attacker may act like the marketing director and then send email to a departmental project manager (PM) using a subject line that reads, Updated invoice for Q3 campaigns.
- The text, style, and included logo duplicate the organization’s standard email template.
- A link in the email redirects to a password-protected internal document, which is in actuality a spoofed version of a stolen invoice.
- The PM is requested to log in to view the document.
- The attacker steals his/her credentials, gaining full access to sensitive areas within the organization’s network.

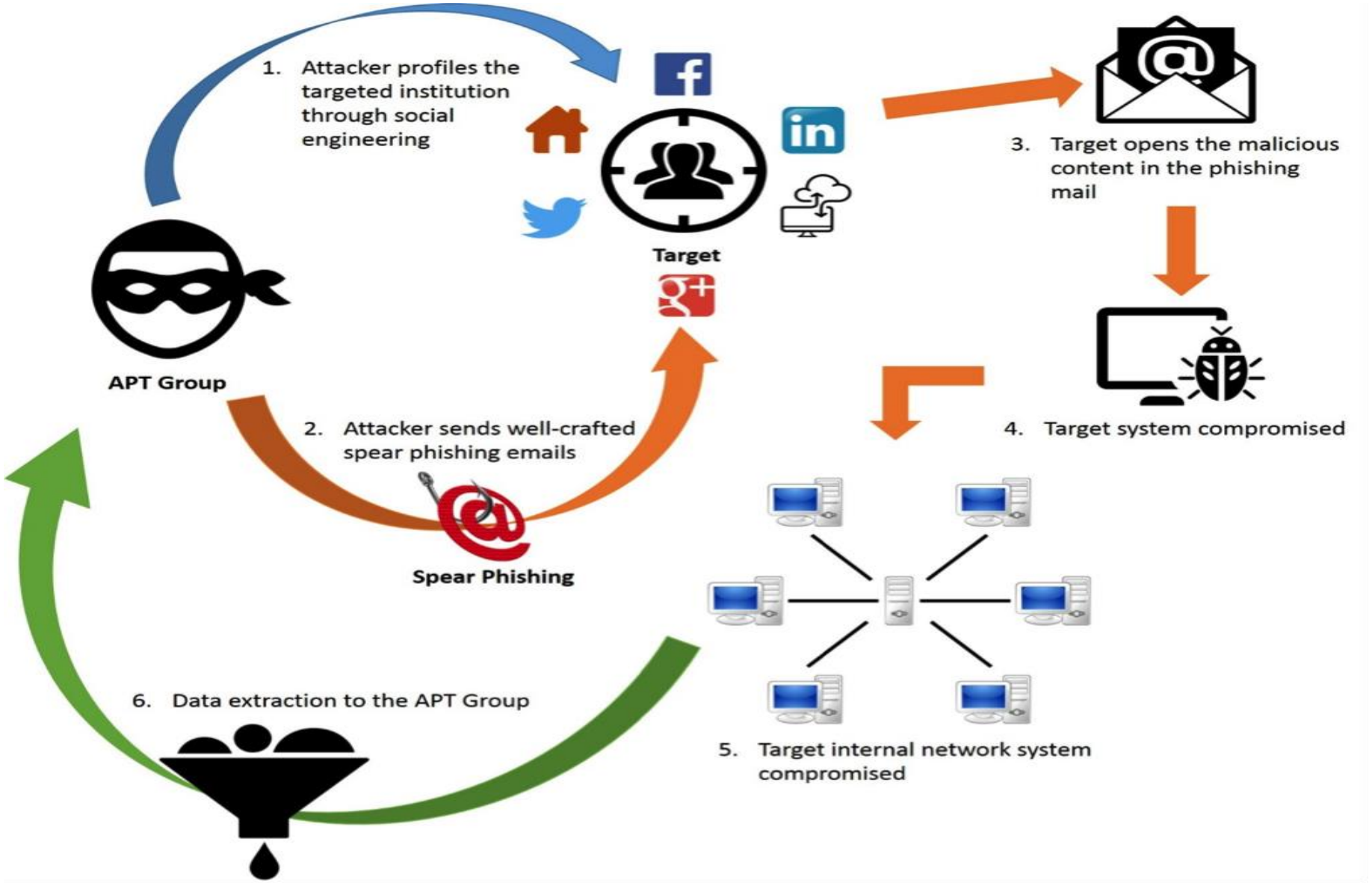

Fig. Spear phishing attack (source: https://resources.infosecinstitute.com)

Phishing attack prevention

- Phishing attack protection requires steps be taken by both users and enterprises.
- For users, vigilance is key.
- A spoofed message often contains subtle mistakes that expose its true identity.

Phishing attack prevention

- These can include spelling mistakes or changes to domain names, as seen in the earlier URL example.
- Users should also stop and think about why they’re even receiving such an email.

Phishing attack prevention

Some phishing prevention methods are:

- Two-factor and three factor authentication methods are the most effective method for countering phishing attacks, as it adds an extra verification layer when logging in to sensitive applications.
- It relies on users having two or three things: something they know, such as a password and user name, something they have, such as their smartcard/smartphones and something they are, such as their biometric information.

Phishing attack prevention

- Organizations should enforce strict password management policies.
- For example, employees should be required to frequently change their passwords and to not be allowed to reuse a password for multiple applications.
- Mandatory use of One Time Password (OTP) mechanism.
- Don’t respond to fake calls.

Phishing attack prevention

- **Awareness-** Educational campaigns can also help to prevent phishing attacks by enforcing secure practices, such as not clicking on external email links.

References

- Textbook: Cyber Security: Understanding Cyber Crimes, Computer Forensics And Legal Perspectives by Sunit Belapure and Nina Godbole
- Michael E. Whitman and Herbert J. Mattord, Principles of Information Security, (2e), Thomson Learning, 2007