

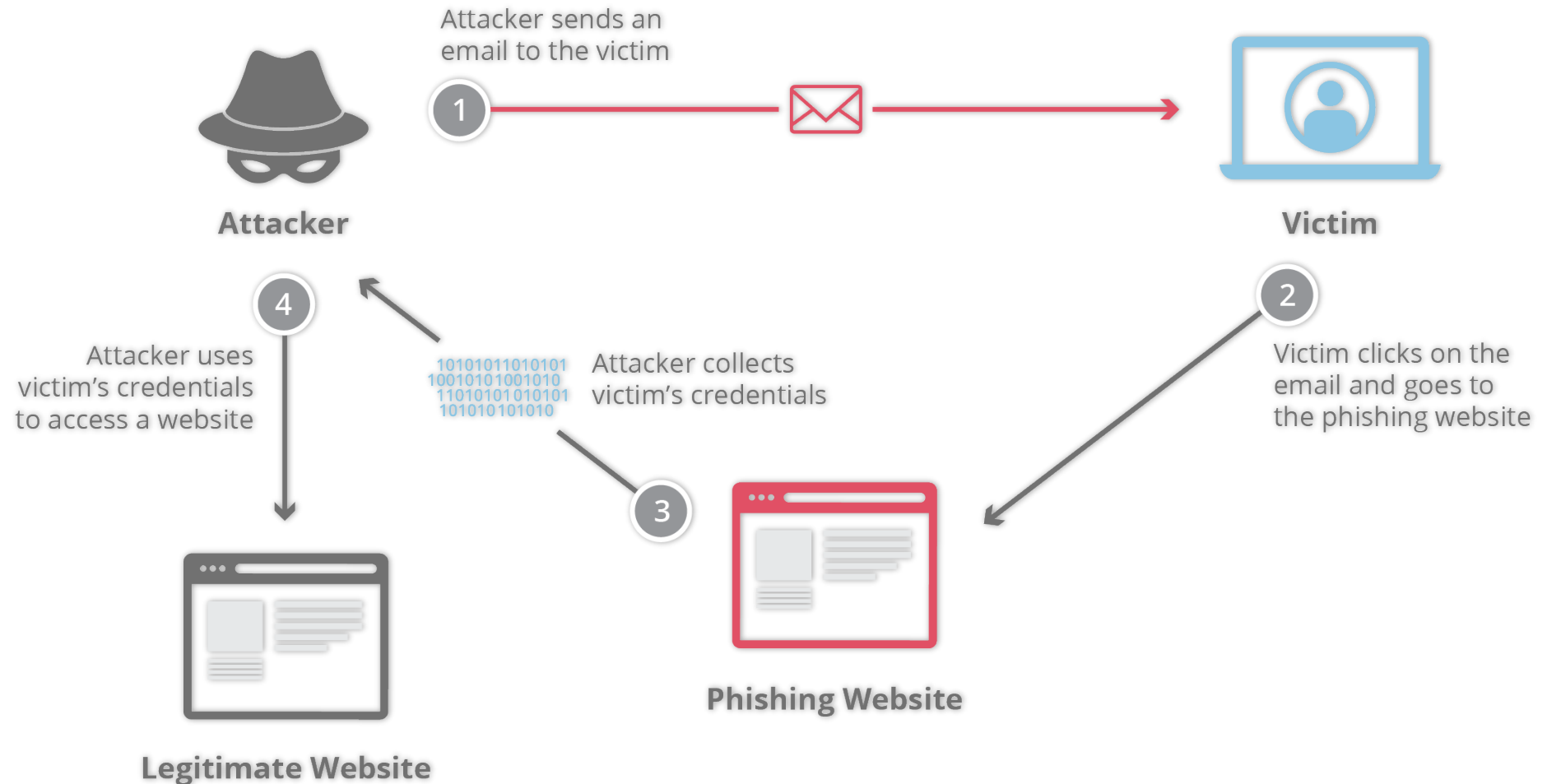
Social Engineering

Dr. Shahzada Khurram

Phishing (Social engineering email attack):

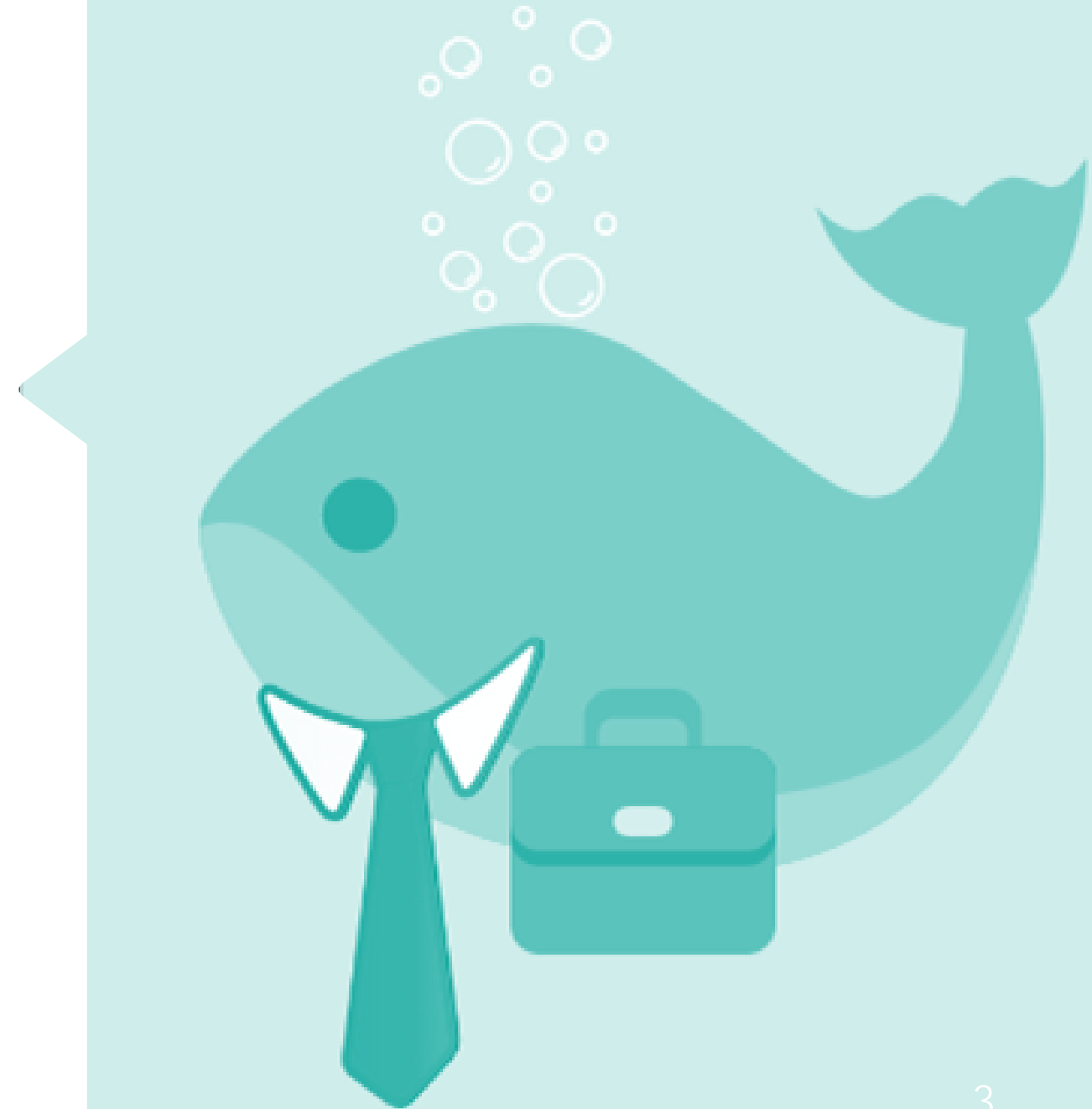
Click to win, Send information to get your inheritance ...

Sent to hundreds of thousands of people; if just 0.02% follow the instructions they have 200 victims.



Spear Phishing and Whale Phishing

- **Spear Phishing:** Targeted phishing, not just random spam, but targeted at specific individuals.
 - Sent with knowledge about the target (person or company); familiarity increases success.
- **Whale Phishing (Whaling):** Spear phishing targeted at senior leadership of an organization.
 - This could be: "Your company is being sued if you don't fill out the attached documents (with trojan in them) and return them to us within 2 weeks".



Tailgating or “piggybacking”

In these types of attacks, someone without the proper authentication follows an authenticated employee into a restricted area. The attacker might impersonate a delivery driver and wait outside a building to get things started. When an employee gains security's approval and opens the door, the attacker asks the employee to hold the door, thereby gaining access to the building



Vishing (Voice Phishing)

○ Attacks over automated VOIP (Voice over IP) systems, bulk spam similar to phishing.

○ These are: "Your taxes are due", "Your account is locked" or "Enter your PII to prevent this" types of calls.

1. I'm calling from your bank. For your account security, I need you to give me the 6-digit passcode we just texted to you.
2. We just want to verify our information (most often claiming to be your insurance company).
3. There's a lawsuit against you/warrant for your arrest for tax evasion.
4. You just need to pay shipping and handling (or a small fee) to receive your prize.



Don't become a victim

- While phishing attacks are rampant, short-lived, and need only a few users to take the bait for a successful campaign, Tips to Remember:
 - **Slow down.** Spammers want you to act first and think later. If the message conveys a sense of urgency or uses high-pressure sales tactics be skeptical; never let their urgency influence your careful review.
 - **Research the facts.** Be suspicious of any unsolicited messages. If the email looks like it is from a company you use, do your own research. Use a search engine to go to the real company's site, or a phone directory to find their phone number.
 - **Don't let a link be in control of where you land.** Stay in control by finding the website yourself using a search engine to be sure you land where you intend to land. Hovering over links in email will show the actual URL at the bottom, but a good fake can still steer you wrong.
 - **Email hijacking is rampant.** Hackers, spammers, and social engineers taking over control of people's email accounts (and other communication accounts) has become rampant. Once they control an email account, they prey on the trust of the person's contacts. Even when the sender appears to be someone you know, if you aren't expecting an email with a link or attachment check with your friend before opening links or downloading.
 - **Beware of any download.** If you don't know the sender personally AND expect a file from them, downloading anything is a mistake.
 - **Foreign offers are fake.** If you receive an email from a foreign lottery or sweepstakes, money from an unknown relative, or requests to transfer funds from a foreign country for a share of the money it is guaranteed to be a scam.

Ways to Protect Yourself

- **Delete any request for financial information or passwords.** If you get asked to reply to a message with personal information, it's a scam.
- **Reject requests for help or offers of help.** Legitimate companies and organizations do not contact you to provide help. If you did not specifically request assistance from the sender, consider any offer to 'help' restore credit scores, refinance a home, answer your question, etc., a scam.
Similarly, if you receive a request for help from a charity or organization that you do not have a relationship with, delete it. To give, seek out reputable charitable organizations on your own to avoid falling for a scam.
- **Set your spam filters to high.** Every email program has spam filters. To find yours, look at your settings options, and set these to high—just remember to check your spam folder periodically to see if legitimate email has been accidentally trapped there.
- **Secure your computing devices.** Install anti-virus software, firewalls, email filters and keep these up-to-date. Set your operating system to automatically update, and if your smartphone doesn't automatically update, manually update it whenever you receive a notice to do so.

Thank you