PHISHING AWARENESS TRAINING

Phishing Exposed: Building Awareness and Resilience in the Digital Age"

TABLE OF CONTENT

PHISHING ATTACKS

What is Phishing?

Phishing is a cyberattack where attackers use fraudulent emails, messages, phone calls, or websites to trick individuals into revealing sensitive data, downloading malware, or otherwise exposing themselves to cybercrime .

Concept Of Phishing- The Art Of Digital Deception

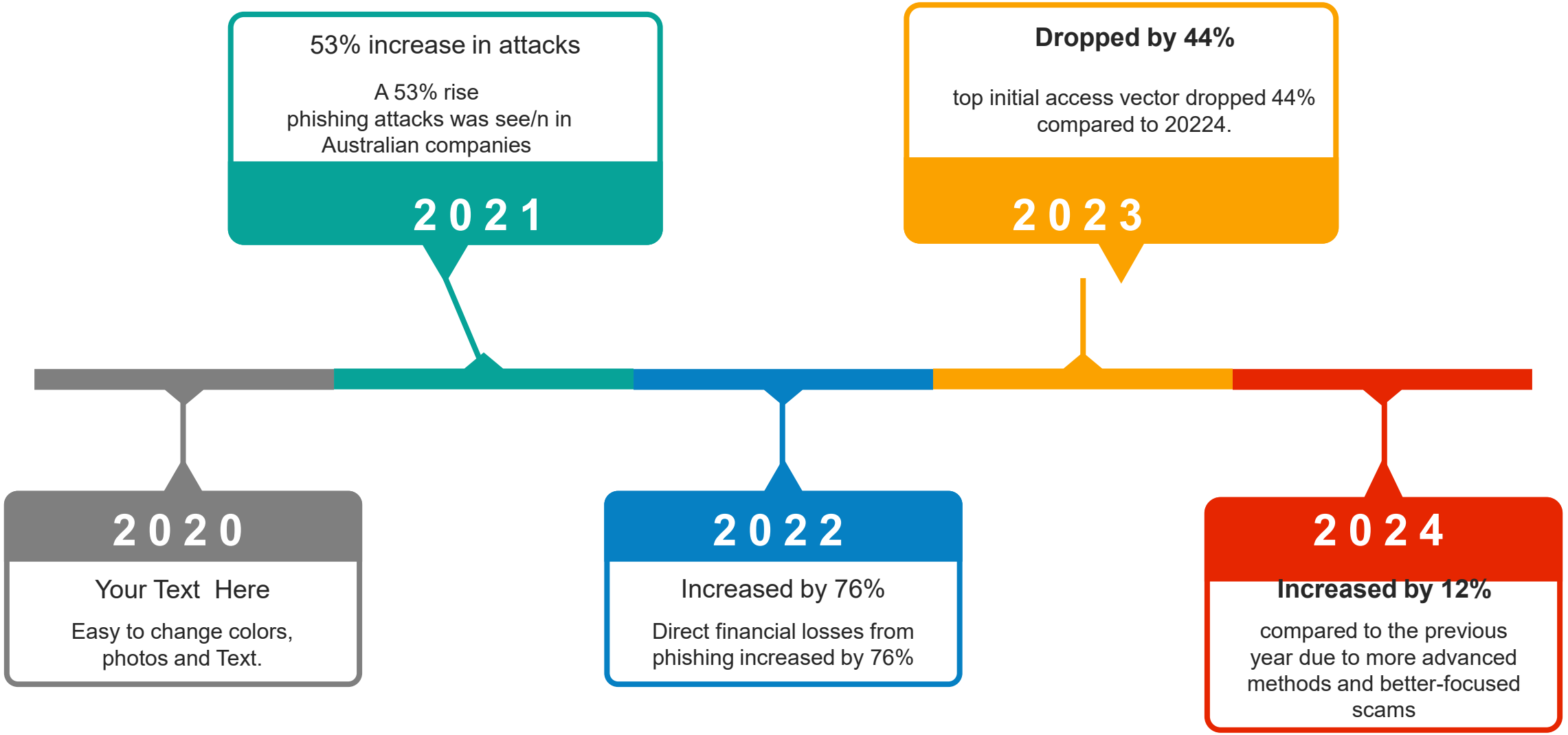
In Phishing, attackers attempt to trick individuals into revealing sensitive information, such as usernames, passwords, credit card numbers, or other personal data, or to execute actions (like clicking a malicious link or opening an infected attachment).

The attacker achieves this by masquerading as a trustworthy entity in an electronic communication.

Why Phishing?

- Financial gain
- Data theft
- Malware Delivery
- Disruption/Sabotage

Timeline Style



PHISHING EMAIL INDICATORS

Think of your inbox as a fishing pond, and every email is a potential lure. Before you bite, inspect the bait.

01

Scrutinize the Sender (The "From" Field)

- Look beyond the displayed name
- Check for Typos
- Be Wary of Generic Senders

02

Inspect the Email Content

- Generic Greetings
- Grammar and Spelling
- Look for Mismatches

03

Analyze the Subject Line

- Sense of Urgency or Threat
- Suspicious Attachments
- Too Good to Be True

04

Pressure to Act Quickly

VERIFYING WEBSITE AUTHENTICITY

1. Check the URL
- ✓ For instance; checking for the exact correct domain, the actual domain name is the part before t the first single slash / after https://
- ✓ Watch for Typosquatting ; gØØgle.com instead of google.com
- ✓ **Look for the padlock icon** in the address bar. This shows encrypted connection

2. Check website design and content
- ✓ Poor quality
- ✓ Missing Information
- ✓ Suspicious Prompts

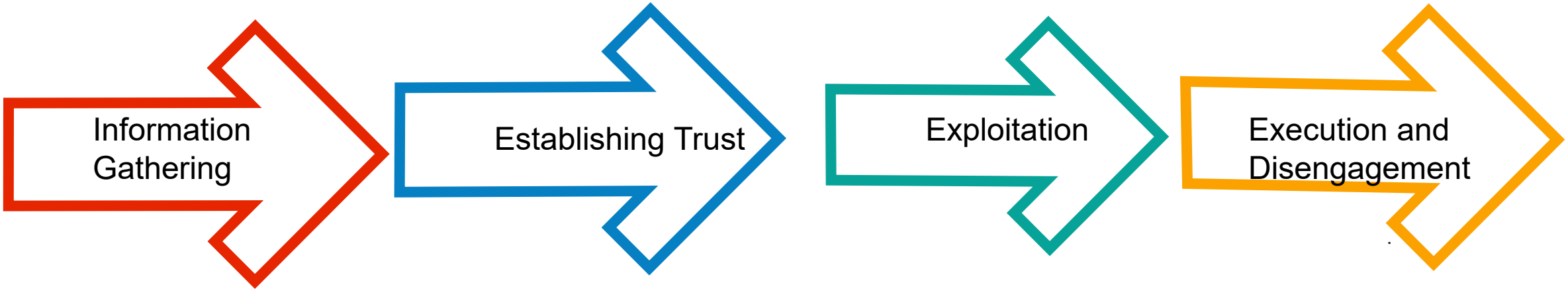
3. Check for Interactivity and Functionality

4. Use External Verification
- ✓ Contact directly
- ✓ Google Search

SOCIAL ENGINEERING

Social engineering is a non-technical method of intrusion that relies on human interaction and psychological manipulation. Attackers exploit natural human tendencies (trust, curiosity, fear, helpfulness, urgency) to trick victims into breaking normal security procedures.

ATTACK CYCLE



Common Social Engineering Attack Vectors & Techniques

Phishing (Email/SMS/Voice): Deceptive communications sent from seemingly trustworthy sources to trick recipients into revealing sensitive information

Baiting: Luring victims with a promise of something desirable (free movie, USB drive with "important data") in exchange for giving up information or infecting their system.

Dumpster Diving: Sifting through discarded physical documents (trash) to find sensitive information that can be used for other social engineering attacks or direct data theft.

Ailgating (Piggybacking): Gaining unauthorized access to a restricted area by following closely behind someone who has legitimate access

Impersonation and Deepfakes: Attackers pretend to be someone else, including using AI-generated audio or video (deepfakes) to convincingly mimic executives or colleagues23.

Best Practices and Tips to Avoid Falling Victim

01

Be Skeptical and Verify Requests

Question unexpected requests for sensitive information or urgent actions

02

Limit What You Share Online

Avoid oversharing personal or work information on social media, as attackers use these details to craft convincing scams

03

Use Strong Passwords and Enable Multi-Factor Authentication

Create unique, complex passwords for every account and enable MFA to add an extra layer of security

04

Keep Software Updated

Regularly update your devices, software, and security patches to close vulnerabilities that attackers may exploit.

05

Think Before Clicking

Don’t click on links or download attachments from unknown sources. Hover over links to check their legitimacy.

Real-World Social Engineering Examples

Google and Facebook $100 Million Scam:

Attackers impersonated a legitimate supplier and sent fake invoices to employees at Google and Facebook, tricking them into transferring over $100 million to fraudulent accounts. The emails looked authentic and referenced real business relationships, bypassing standard verification steps

Twitter 2020 Breach

Hackers used vishing (voice phishing) to pose as IT staff, convincing Twitter employees to provide access credentials. This allowed attackers to take over high-profile accounts, including those of Elon Musk and Barack Obama, and post cryptocurrency scams..

Ubiquiti Networks $46.7 Million Loss

An attacker pretended to be a senior executive and emailed the finance team, instructing them to transfer funds to an overseas account. The realistic pretext and urgency led to a $46.7 million loss

Vendor Payment Scam (Pretexting)

An accounts payable employee received a call from a “vendor” claiming their banking details had changed. The scammer was friendly and convincing, ultimately persuading the employee to update payment information and send funds to the attacker’s account.

Interactive Quizz Questions

1. You get a call from “IT support” asking for your password to fix a system issue. What should you do?

a) Give them your password
b) Hang up and report the call
c) Ask them to email you instead.

2. You find a USB drive labeled “Employee Salaries” in the office parking lot. What’s your next move?

a) pug it in to see what’s inside
b) Hand it to your IT/security team
c) Take it home for later

3. A pop-up says you’ve won a new phone and asks for your company login. What should you do?

a) Enter your credentials to claim the prize
b) Close the pop-up and report it
c) Forward the link to your friends

5. Which of these is NOT a social engineering tactic?

a) Phishing
b) Tailgating
c) Firewall configuration


THANK YOU