Attacks, Threats, and Vulnerabilities for CompTIA Security+

COMPARING DIFFERENT TYPES OF SOCIAL ENGINEERING TECHNIQUES

Module Overview

What is social engineering?

- Why is it so effective?

Social engineering techniques

- Various techniques (phishing, smishing, vishing)
- Shoulder surfing, dumpster diving

Influence Campaigns

- Hybrid warfare

Reasons for effectiveness

- Authority, intimidation, trust, etc.

What is Social Engineering?

Social Engineer is a master of asking seemingly non-invasive or unimportant questions to gather information over time

- Gain trust
- Reduce defenses

Can be combined with a number of techniques to gather sensitive information

Phishing

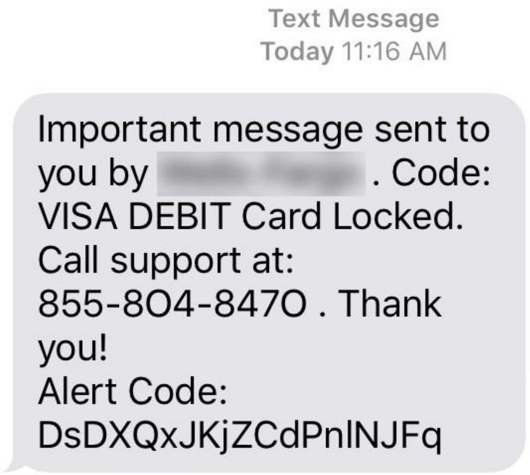
- Obtaining sensitive information (usernames, passwords, credit card info)
- Tricking a user into entering their info into a fake website
  - Email spoofing
  - Instant messaging
  - SMS (Smishing)
- Pretend to be social media websites, auction sites, or communications from friends or colleagues

Types of Phishing

Spear Phishing
Like phishing, except the target is well researched and appears to come from a trusted sender

Whaling
Phishing campaigns that target the “big fish” within an organization, for things like wire transfers, tax information and other financial data

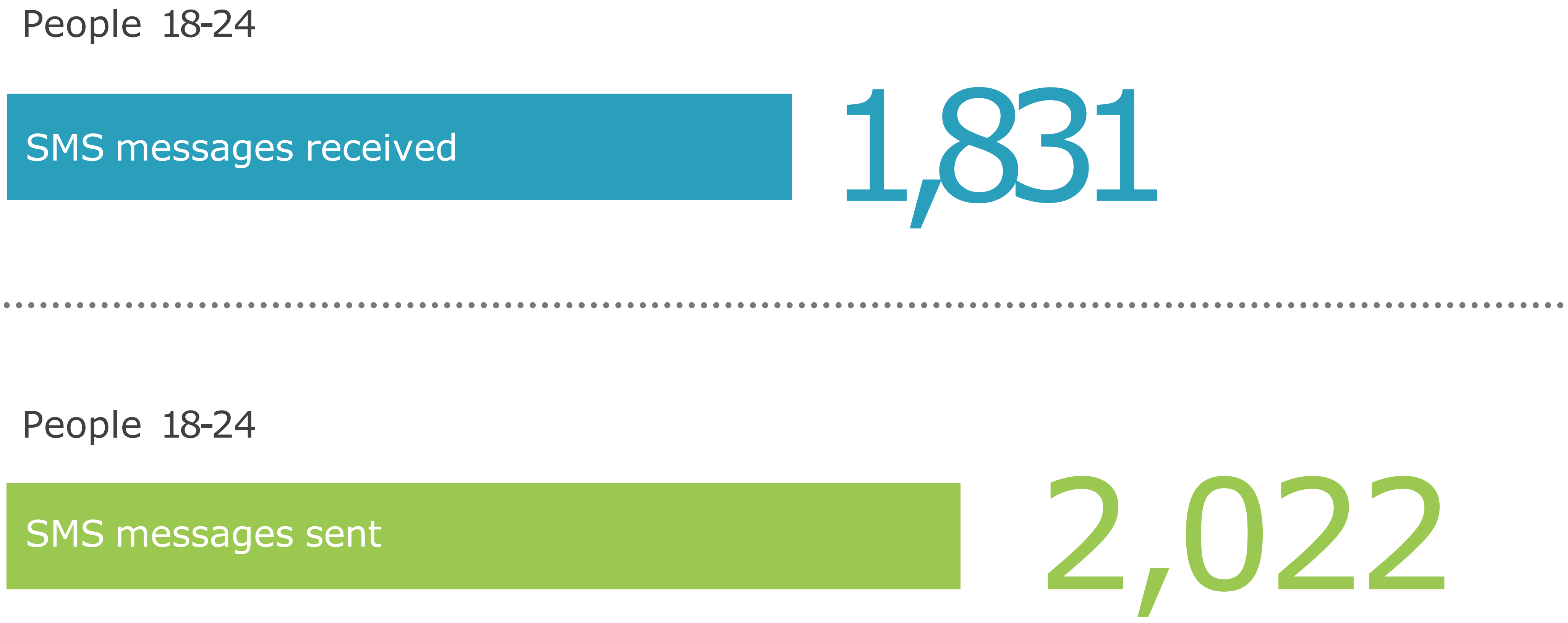
Smishing
Phishing attacks carried over SMS



Text Message
Today 11:16 AM

Important message sent to you by [redacted] . Code: VISA DEBIT Card Locked. Call support at: 855-8O4-847O . Thank you!
Alert Code: DsDXQxJKjZCdPnINJFq

Smishing (SMS Phishing)



People 18-24

SMS messages received

1,831

People 18-24

SMS messages sent

2,022

Recent study by Experian.com

Smishing (SMS Phishing)

People 45-54

SMS messages received

473

People 45-54

SMS messages sent

525

Recent study by Experian.com

6 billion texts are sent every day *in the U.S. alone*

27 trillion texts are sent every year

Vishing

Voice Phishing

Social Engineering techniques designed get the victim to divulge personal or sensitive information

Attacker poses as legitimate company, repair person, security personnel or someone of trust

- Internal or external to the company

SPAM

Sending of large quantities of unsolicited emails

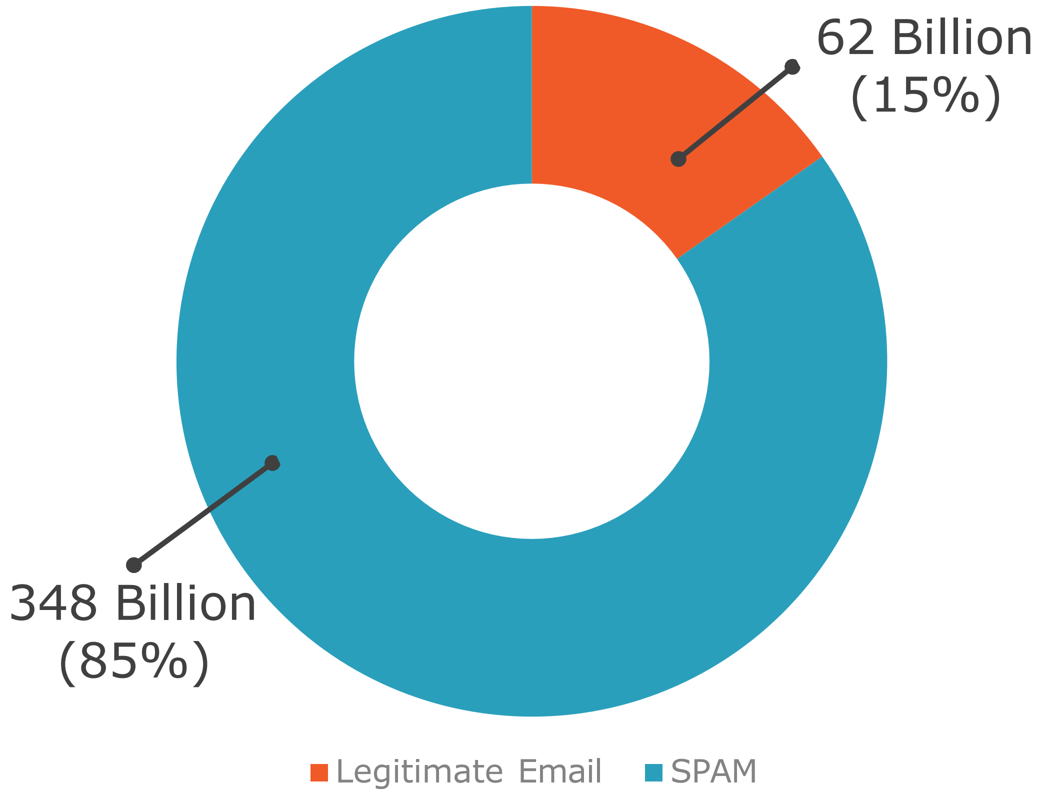
- Typically for commercial advertising
- Can also be used via social media, texts/IM, video and VoIP spam

SPAM over Instant Messaging (SPIM)

- Can be more effective as the interactions can occur in real-time

SPAM (How Bad is It?)

Emails Sent per Day (in Billions)



- Cloud email services continually get better at catching spam
- It’s a “shotgun” approach and primarily a numbers game
- Extremely important to continually educate users NOT to click on links, and use common sense
- Some SPAM is caught by keywords, content, originating domain or IP address/range

Dumpster Diving

Removing trash from dumpsters that could reveal sensitive information

- Usernames/passwords
- Personally Identifiable Information (PII)
- Company documents, resumes, etc.

Dumpster Diving

Mitigation

- Shredding documents prior to disposal
- Locked waste cans to be transported off-site for shredding/disposal

Shoulder surfing

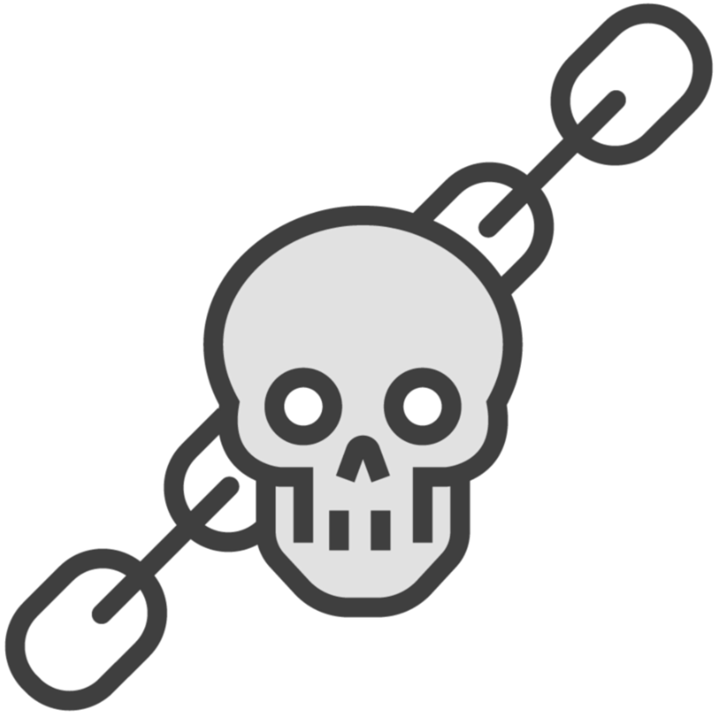
Social engineering trick to get someone to enter credentials into an application or website

- Strike up a conversation about their kid's sports, then ask to see some pictures
- Should surf as they enter their username/password into social media website

Shoulder surfing mitigation

- Privacy screens
- Masked passwords
  - Multiple asterisks per keystroke further obfuscates the length of a password
- Technical Controls
  - Cameras to monitor doors, sensitive areas, key card access, etc

Pharming

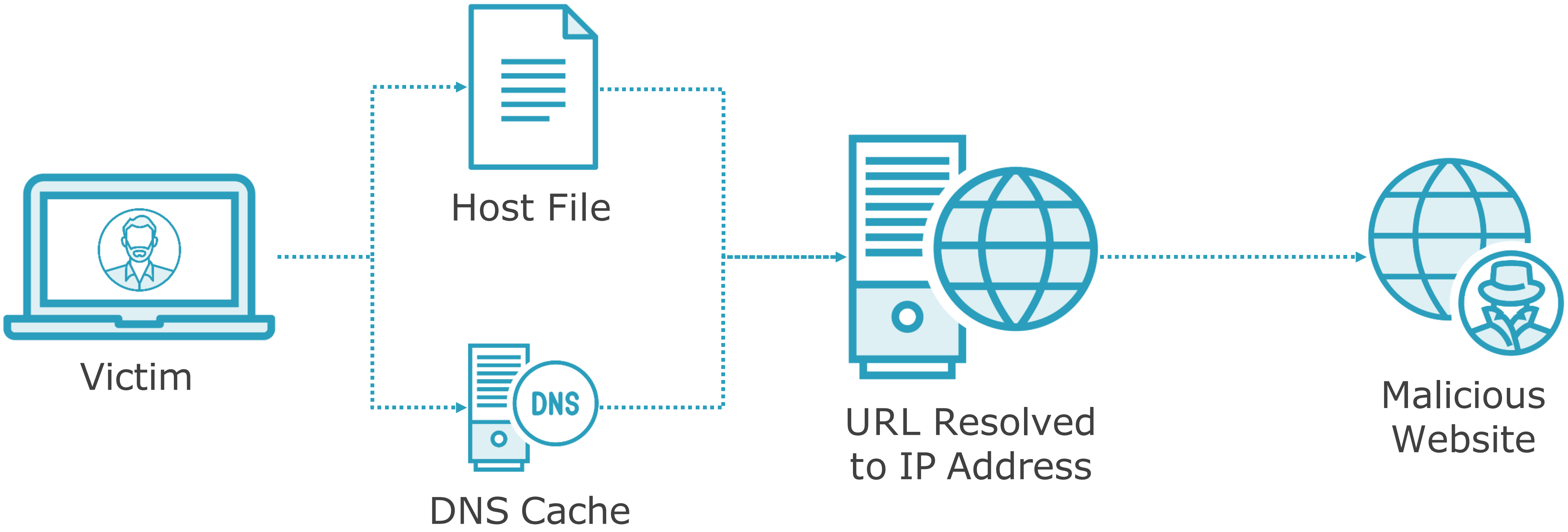


Redirecting a user’s website traffic to a fake, malicious website

- DNS cache poisoning
- Host file injection

User visit’s fake website and enters credentials (username, password, etc.)

Pharming



All these types of attacks are designed to elicit information from the user

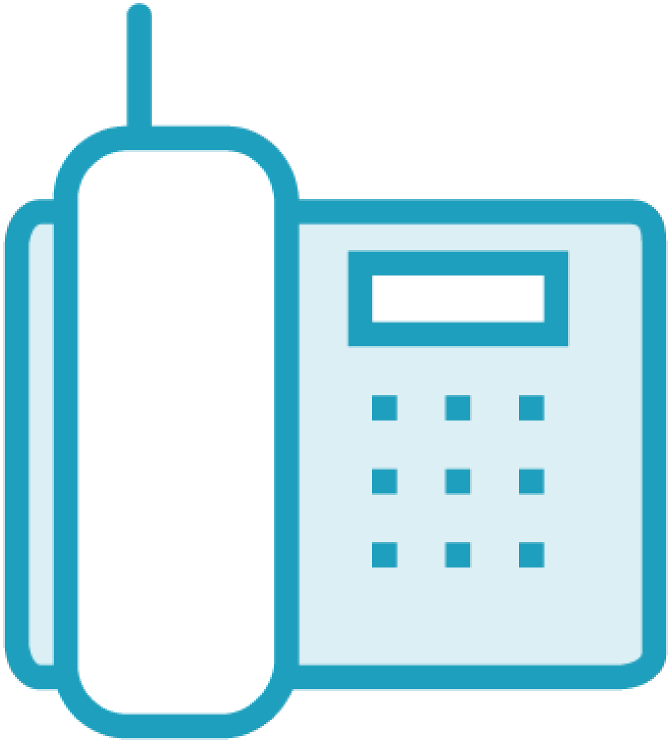
Tailgating

Following someone into a building through a gated area or badged access area

- People want to be helpful
- Bad actors know that people will hold the door for people who look like they belong
  - Carrying lots of items, etc.

Training and understanding of corporate policy is key

Hoaxes



Social engineering technique using the phone and/or voicemail to trick the target into providing sensitive information

- Hacker acts like remote technician or employee
- Interested party seeking employment
- Angry customer filing complaint

Hoaxes

Targeted phishing and spear phishing techniques aimed at “big fish” like company executives (i.e. “whaling”)

- Phishing, vishing and various social engineering techniques to gather information
- Emails are targeted, very specific and seem legitimate

Hoaxes

Security Awareness Training

- Ensure employees know to never click links from sources they don't know
- Don't open attachments from an unknown origin

Technical Controls

- SPAM filtering
- Heuristics
- Firewalls / Deep Packet Inspection

Prepending

Adding mentions (@username) to tweets or social media posts to make them seem more personal

- Higher engagement
- Can be automated to become almost as efficient as manual spear-phishing campaigns

Impersonation

Impersonation can be done via a number of methods:

- Social engineering
- Stolen credentials / credential harvesting
- Infiltrating a network and capturing and replaying packets on a network

Identity Fraud

Identity theft and identity fraud are interchangeable terms

- Malware, social engineering, and old-school methods (i.e. dumpster diving)
- Victim’s identity is used to obtain credit, steal money/assets, etc.

Invoice Scams

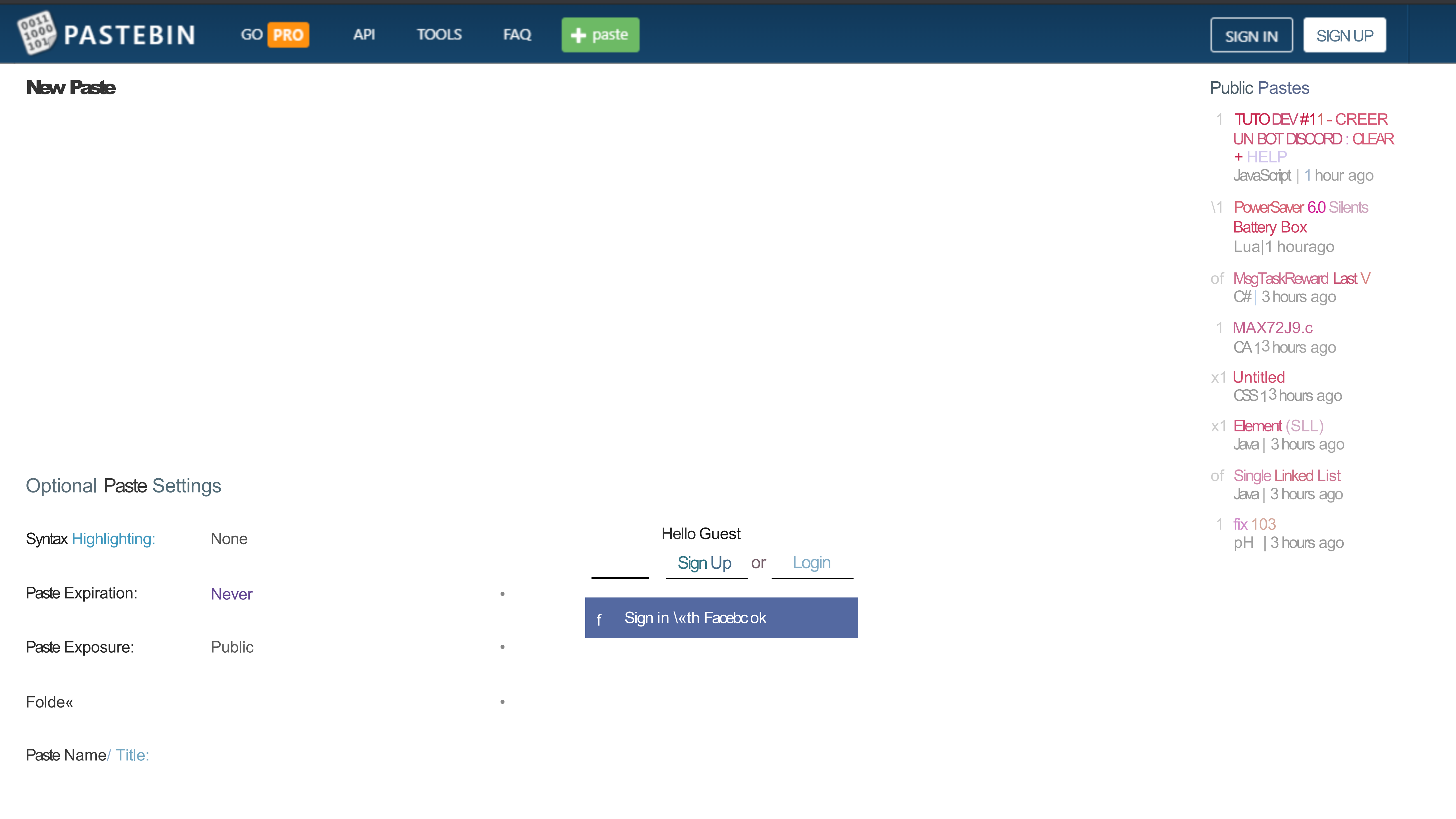
- “Whaling” technique where bad actors spoof executive email accounts
- Contact finance and/or accounts payable and ask them to pay a fraudulent invoice
  - Wire transfer
  - Company credit card
  - Cryptocurrency

Credential Harvesting

Phishing campaigns
Phishing, smishing, SPAM/SPIM, etc., can be used to gather user's credentials at scale

Malware
Can be used to target an individual victim, or entire websites and networks.   Credentials are often harvested and sold or pasted online

Pastebin and other paste sites
Paste sites allow hackers and bad actors to post large amount of comprised accounts and information, as well as access other breach information



New Paste

Public Pastes

1 TUTO DEV #11 - CREER UN BOT DISCORD : CLEAR + HELP
JavaScript | 1 hour ago

\1 PowerSaver 6.0 Silents Battery Box
Lua|1 hourago

of MsgTaskReward Last V
C# | 3 hours ago

1 MAX72J9.c
CA 13 hours ago

x1 Untitled
CSS 13 hours ago

x1 Element (SLL)
Java | 3 hours ago

of Single Linked List
Java | 3 hours ago

1 fix 103
pH | 3 hours ago

Optional Paste Settings

Syntax Highlighting: None

Paste Expiration: Never

Paste Exposure: Public

Folde«

Paste Name/ Title:

Hello Guest

Sign Up or Login

f Sign in \«th Facebc ok

Watering Hole Attack

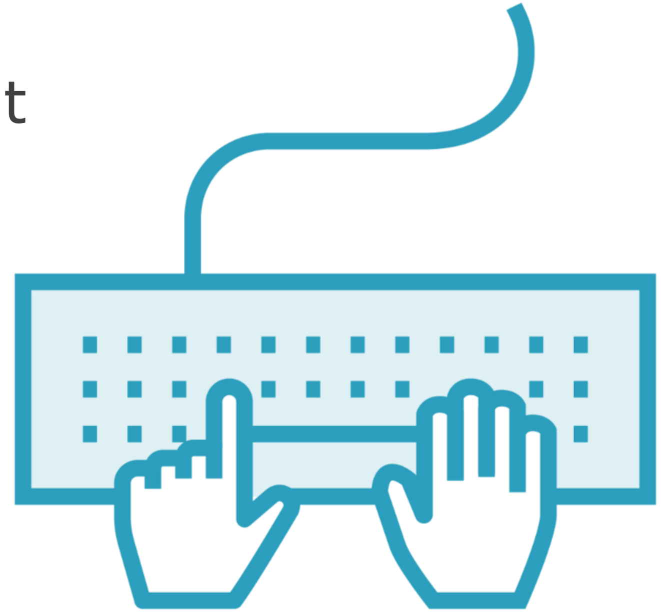
Sophisticated attack that identifies less secure websites that users in the target company or organization are likely to visit

- Attackers plant malware on the site(s) users visit to then infect the targeted users - once they visit the infected site
- Malicious code scans the users’ computer for vulnerabilities, zero-days, etc
  - May download additional code to initiate attacks, siphon data, etc.

Typo Squatting/URL Hijacking

Setting up domain names to capitalize on the fact that users make typos

- Facbook.com instead of Facebook.com
- Goggle, Googel, Googgle, etc



Fraudulent websites that resemble the real ones

- Capture user credentials

Ad portals full of ads that might appeal to a user going to that website

- Hoping to create ad revenue by supplying complementary advertising

Hybrid Warfare

Combination of traditional and irregular forces in the same military campaign

- Guerillas, insurgents
- Proxies, terrorists
- State and non-state actors

Aimed at achieving a common political goal

Hybrid Warfare

- Information Operations
- Cyber Activities
- Proxy Organizations
- Economic Influence
- Clandestine Measures
- Political Influence

Social Media

Influence campaigns

- Social media can be extremely powerful in shaping public opinion
  - Helping or hurting company image, stock price, consumer confidence
  - Public policy, elections, attitudes toward government, law enforcement, etc.

Principles (Reasons for Effectiveness)

- Authority
- Intimidation
- Consensus/ Social Proof
- Familiarity/Liking
- Trust
- Scarcity/Urgency

Authority

Bad actor appears to know what they’re talking about or has special knowledge of the company

Position of authority (executive or upper management)

- Technical jargon
- Name dropping
- Knowledge of specific systems / applications

Intimidation

Social engineer can use several techniques (i.e. authority, trust) to then impose their will on the target

- Threaten negative action
- Threaten to release sensitive information
- Can be combined with scarcity/urgency

Consensus/Social Proof

People are more likely to act when they believe they are in alignment with the larger group

- “Mob Mentality”
- Bartender who seeds his tip jar
- Review on shopping sites (“4 1/2 Stars” on Amazon, etc)

Familiarity/Liking

People like using or buying things they are already familiar with and like

Likely to converse with people they perceive to "be like them"

Attacker will establish a common contact or friend

- Trust goes up when people think they're dealing with someone with mutual friends or contacts

Trust

People are more likely to act when they trust the person or situation

Social engineers can use a variety of tactics to shortcut the path to trust

- Authority
- Familiarity/company specific jargon
- Name dropping
- Shoulder surfing / dumpster diving

Scarcity / Urgency

Social engineering tactics to elicit action by making the target think they have to act quickly to take advantage of a special deal, pricing, etc

- Victim feels they must act quickly or risk missing out
  - Dwindling stock
  - Time-based offer
  - Issue(s) that need to be resolved quickly

Module Review

What is social engineering?

- Why is it so effective?

Social engineering techniques

- Various techniques (phishing, smishing, vishing)
- Shoulder surfing, dumpster diving

Influence Campaigns

- Hybrid warfare

Reasons for effectiveness

- Authority, intimidation, trust, etc.