9.1 SOCIAL ENGINEERING CONCEPTS

- Social Engineering Concepts
- Human Motivation
- Organizational Vulnerability
- Phases of Social Engineering

Amateurs hack systems,
Professionals hack people.

WHAT IS SOCIAL ENGINEERING?

- The psychological manipulation of people into divulging confidential information or performing actions that they shouldn’t do
- A low-tech way of gaining unauthorized information or access to systems

IMPACT OF SOCIAL ENGINEERING ON AN ORGANIZATION

- Social engineers rely on the fact that people are not aware of the value of their information and don’t protect it properly
- Impact of social engineering attack on an organization includes:
  - Financial loss
  - Loss of privacy
  - Potential terrorism
  - Damaged goodwill
  - Temporary/permanent closure
  - Potential lawsuits/arbitration

HUMAN MOTIVATION FOR FALLING VICTIM

- Fear
- Greed
- Curiosity
- Helpfulness
- Urgency
- Obedience to authority

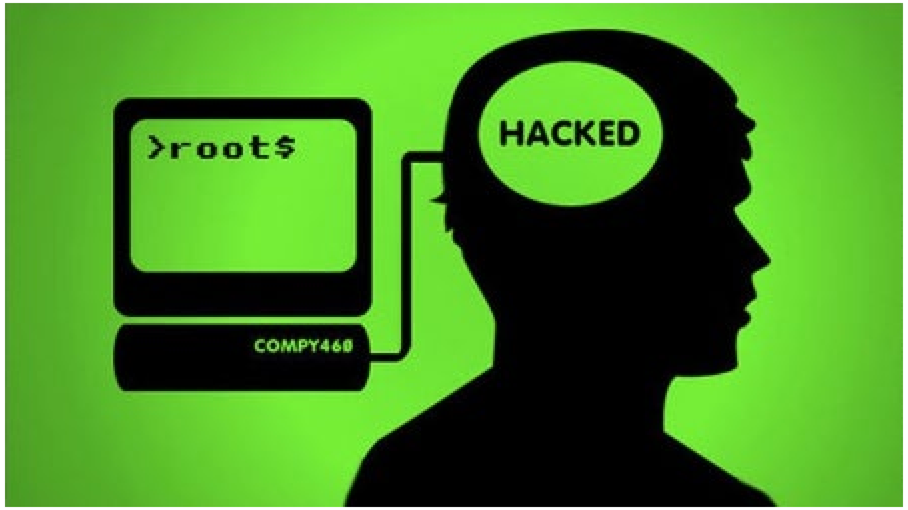
ORGANIZATIONAL VULNERABILITY TO ATTACKS

Reasons organizations can be vulnerable to social engineering attacks:

- Insufficient training in security
- Multiple organizational units/departments
- Access to information isn't regulated
- Insufficient/lack of security policies
- Procedures and protocols that are unclear or not adequately enforced

WHY SOCIAL ENGINEERING IS EFFECTIVE

- Security policies only as strong as weakest link – generally humans
- Social engineering attacks are difficult to detect
- 100% security isn't possible
- Technology cannot adequately compensate for poor judgment



PHASES OF SOCIAL ENGINEERING

- Researching Target Organization
  - Via website, employees, company tour, etc.
- Victim Selection
  - Determine the most vulnerable employees
- Developing Relationship
  - Form a relationship with target employees
- Exploiting Relationship
  - Gather sensitive information and current tech from employees

9.2 SOCIAL ENGINEERING TECHNIQUES

- Common Techniques
- Examples

COMMON SOCIAL ENGINEERING ATTACKS

Attack Type	Description
Impersonation	Calling the victim inside the company or at home and pretending to be someone the user trusts, such as an authority figure or IT support
Pretexting	Giving the victim a (fake) reason for requesting something of them
Quid-pro-quo	Relies on an exchange of information or service to convince the victim to act
Tailgating	An unauthorized person follows an authorized person into the secure or restricted area WITHOUT the knowledge or consent of the authorized person
Piggybacking	An unauthorized person follows an authorized person into the secure or restricted area WITH the consent of the authorized person

Do not confuse tailgating with piggybacking. In tailgating, the attacker slips in behind the authorized user without their knowledge. In piggybacking, the attacker uses social engineering to get the authorized user to hold the door open for them.

COMMON SOCIAL ENGINEERING ATTACKS (CONT'D)

Attack Type	Description
Phishing	• Sending a fake email to a user to entice them into opening a malicious attachment or clicking a malicious link • Typically sent to as many people as possible • Variants include: vishing, smishing, spear phishing, whaling, deep fakes
Spear Phishing	A phishing attack that is targeted towards a specific group
Whaling	A phishing attack that specifically targets a high value person such as a CEO or celebrity
Vishing	• Urgent voice mails or pre-recorded messages that pressure victims into acting quickly to protect themselves from malware, arrest or other risk • A common trick is for a user to dial a number or press a number on their key pad • When the user does so, they are redirected to an expensive pay-by-the-minute phone number that keeps them on hold to incur charges • The charges will appear on their phone bill
Smishing	Phishing using SMS or social media messaging

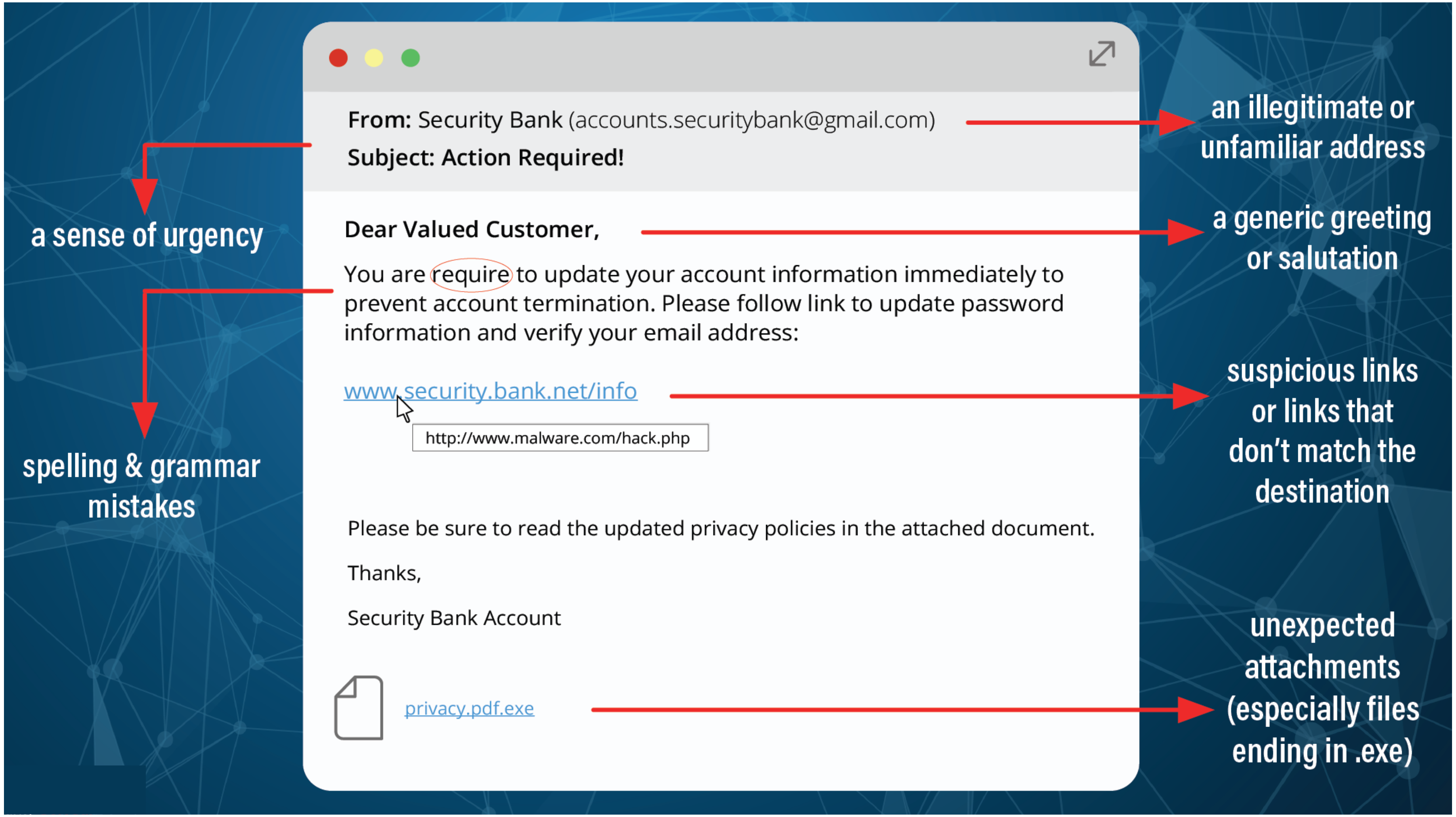
COMMON SOCIAL ENGINEERING ATTACKS (CONT'D)

Attack Type	Description
Water-holing	• Enticing users with a common interest to visit a malicious website • Targeted to a specific group • Often used as a mechanism to gain entry into a specific network
Pharming	• Re-directing a user to a bogus website that mimics the appearance of a legitimate one • Performed through various name resolution attacks such as modifying a HOSTS file, corrupting DNS server or resolver cache, DNS man-in-the-middle, etc. • Done to obtain personal information such as passwords, account numbers, and the like
Clickjacking	• Overlay an invisible (malicious) HTML element on top of a web page • Often a one pixel iFrame • User thinks they are clicking the visible page, but they are also clicking the invisible overlay

COMMON SOCIAL ENGINEERING ATTACKS (CONT'D)

Attack Type	Description
Baiting	Online and/or physical attack that promises the victim a reward
Fake Malware	Victims are tricked into believing that malware is installed on their computer and that if they pay, the malware will be removed
Ransomware	A form of malicious software that encrypts data and then demands a paid ransom for the decryption key
Shoulder Surfing	An unauthorized person spies over your shoulder as you type; can be done directly or across the room with a mobile device and special camera software
Dumpster Diving	Going through someone's trash to find discarded, but still valuable/sensitive information

IDENTIFYING PHISHING



From: Security Bank (accounts.securitybank@gmail.com)

Subject: Action Required!

Dear Valued Customer,

You are require to update your account information immediately to prevent account termination. Please follow link to update password information and verify your email address:

www.security.bank.net/info

http://www.malware.com/hack.php

Please be sure to read the updated privacy policies in the attached document.

Thanks,

Security Bank Account

privacy.pdf.exe

a sense of urgency

spelling & grammar mistakes

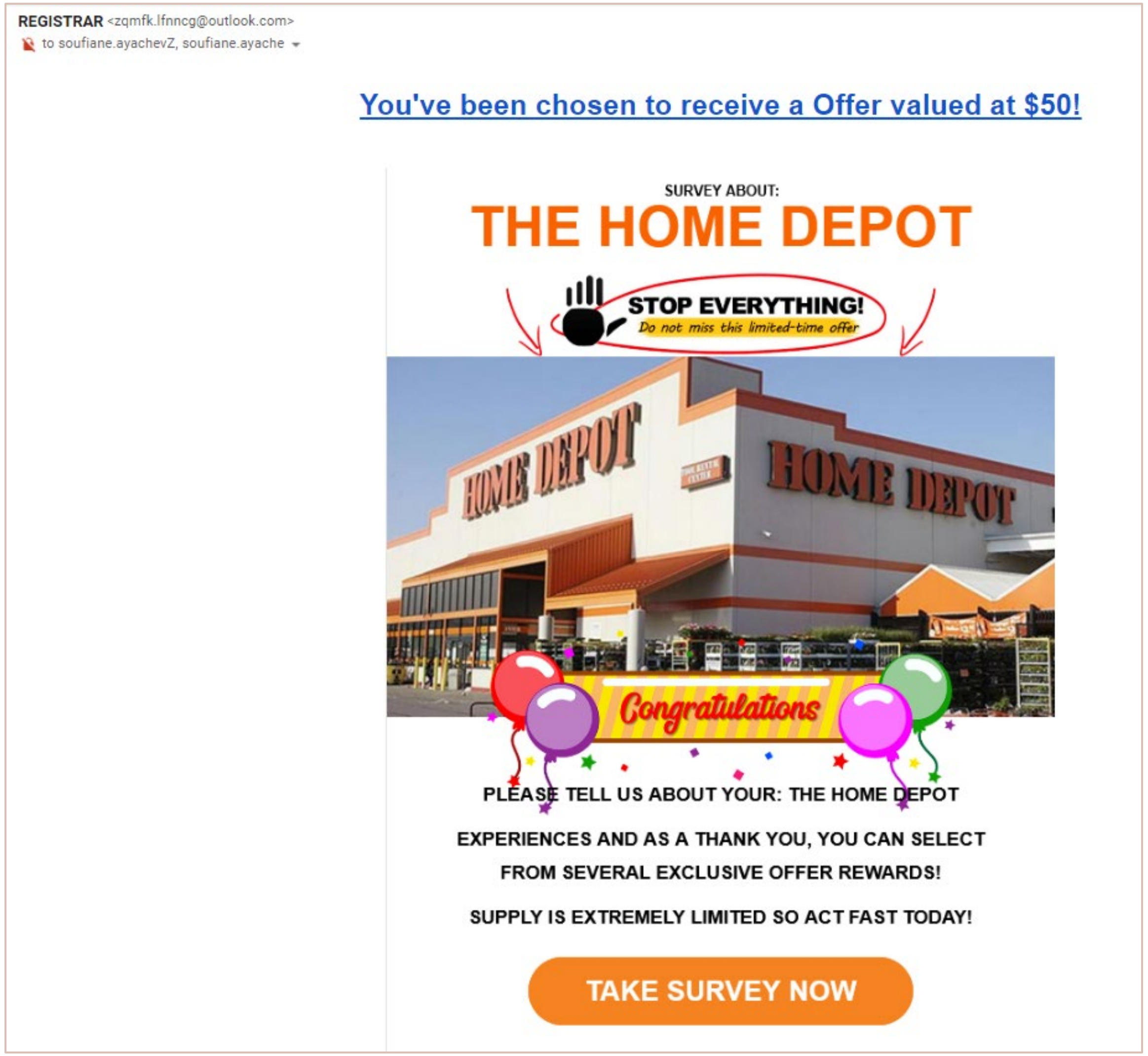
an illegitimate or unfamiliar address

a generic greeting or salutation

suspicious links or links that don't match the destination

unexpected attachments (especially files ending in .exe)

PHISHING EXAMPLES



REGISTRAR <zqmfk.lfnncg@outlook.com>
to soufiane.ayachevZ, soufiane.ayache

You've been chosen to receive a Offer valued at $50!

SURVEY ABOUT:

THE HOME DEPOT

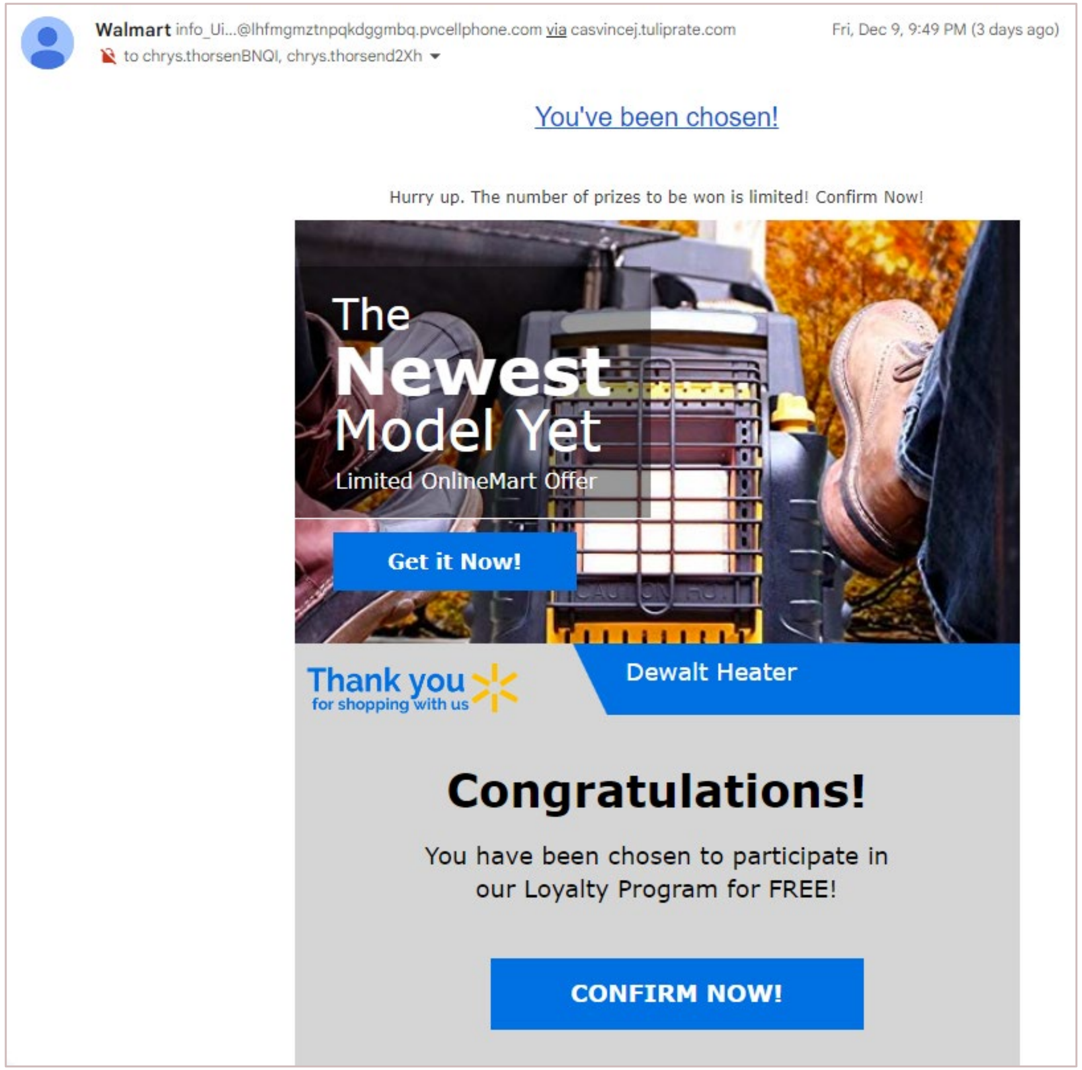
STOP EVERYTHING!
Do not miss this limited-time offer

PLEASE TELL US ABOUT YOUR: THE HOME DEPOT

EXPERIENCES AND AS A THANK YOU, YOU CAN SELECT FROM SEVERAL EXCLUSIVE OFFER REWARDS!

SUPPLY IS EXTREMELY LIMITED SO ACT FAST TODAY!

TAKE SURVEY NOW



Walmart info_Ui...@lhfmgmztnpqkdggmbq.pvcellphone.com via casvincej.tuliprate.com Fri, Dec 9, 9:49 PM (3 days ago)
to chrys.thorsenBNQI, chrys.thorsend2Xh

You've been chosen!

Hurry up. The number of prizes to be won is limited! Confirm Now!

Congratulations!

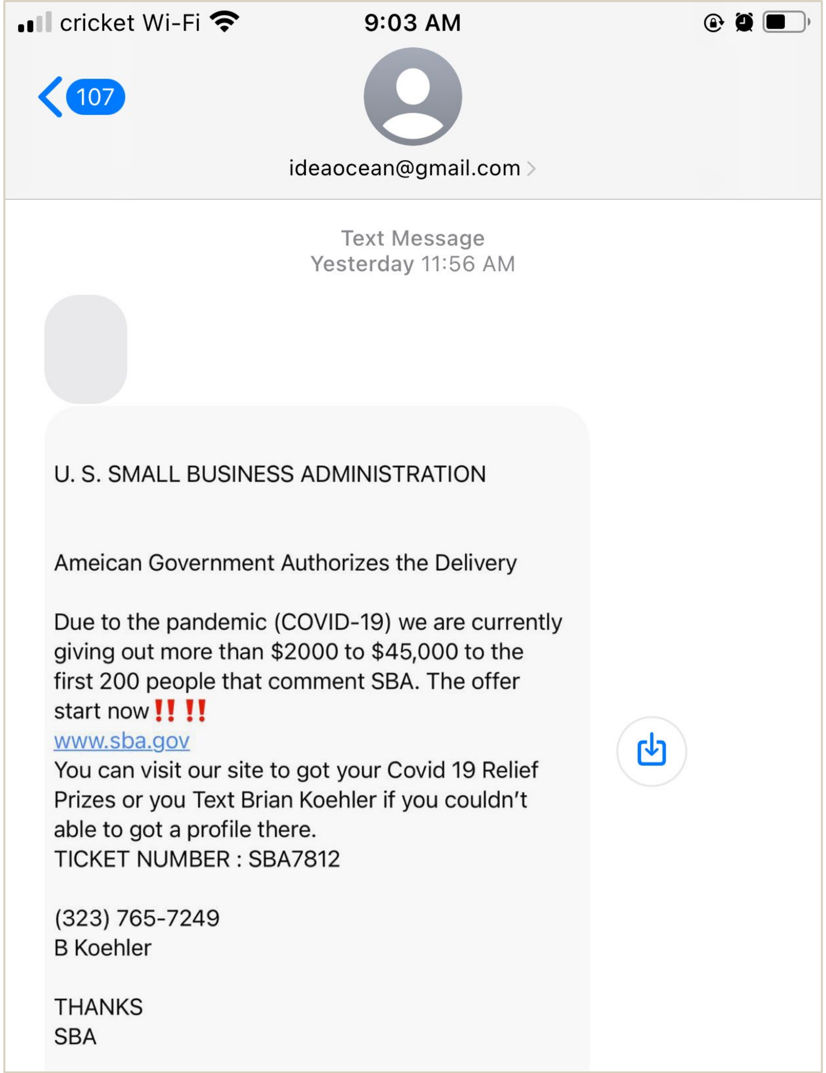
You have been chosen to participate in our Loyalty Program for FREE!

CONFIRM NOW!

SMISHING EXAMPLES

What tells you this SMish is fake?

- The sender is a Gmail account
- Grammar and punctuation errors
- Word choice:
    - Americans tend to refer to their government as "US government"
    - People in some other countries tend to refer to it as "American government"



Text Message
Yesterday 11:56 AM

U. S. SMALL BUSINESS ADMINISTRATION

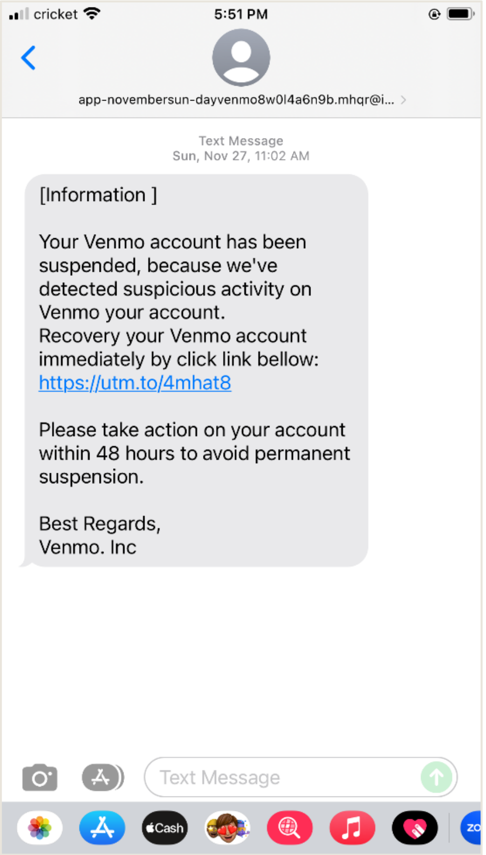
Ameican Government Authorizes the Delivery

Due to the pandemic (COVID-19) we are currently giving out more than $2000 to $45,000 to the first 200 people that comment SBA. The offer start now ‼️ ‼️
www.sba.gov
You can visit our site to got your Covid 19 Relief Prizes or you Text Brian Koehler if you couldn't able to got a profile there.
TICKET NUMBER : SBA7812

(323) 765-7249
B Koehler

THANKS
SBA

SMISHING EXAMPLES #2



app-novembersun-dayvenmo8w0l4a6n9b.mhqr@i...

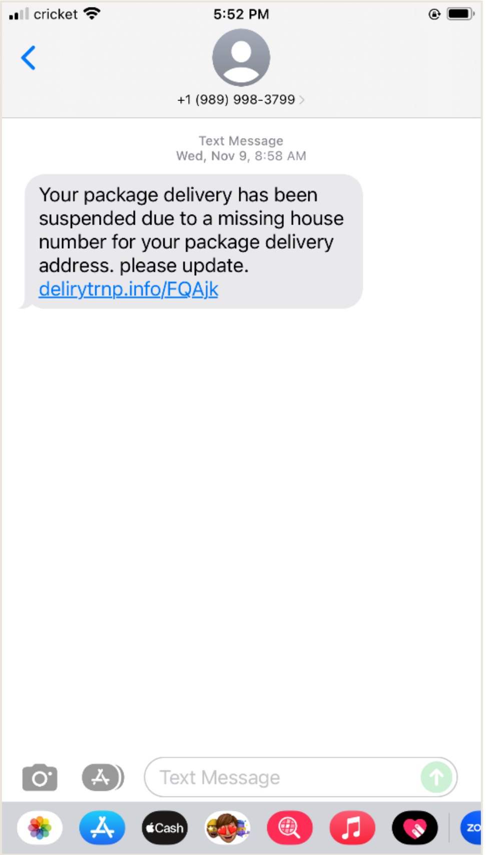
Text Message
Sun, Nov 27, 11:02 AM

[Information]

Your Venmo account has been suspended, because we've detected suspicious activity on Venmo your account.
Recovery your Venmo account immediately by click link bellow:
https://utm.to/4mhat8

Please take action on your account within 48 hours to avoid permanent suspension.

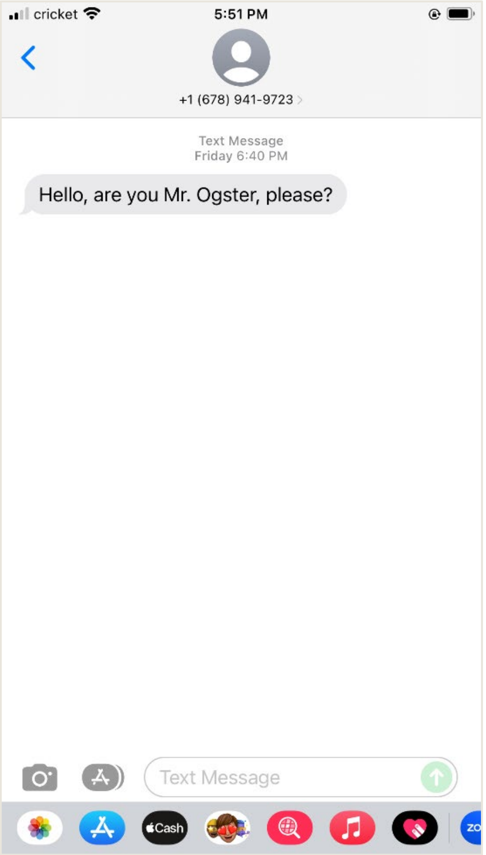
Best Regards,
Venmo. Inc



+1 (989) 998-3799

Text Message
Wed, Nov 9, 8:58 AM

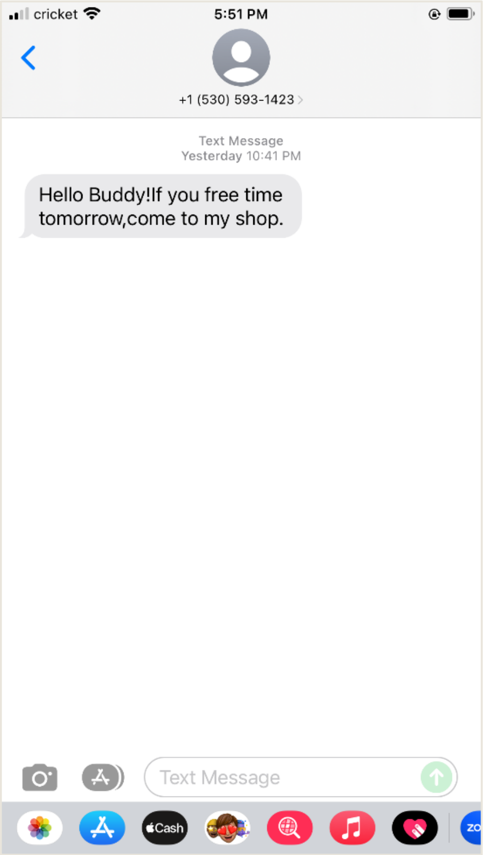
Your package delivery has been suspended due to a missing house number for your package delivery address. please update.
delirytrnp.info/FQAjk



+1 (678) 941-9723

Text Message
Friday 6:40 PM

Hello, are you Mr. Ogster, please?



+1 (530) 593-1423

Text Message
Yesterday 10:41 PM

Hello Buddy!If you free time tomorrow,come to my shop.

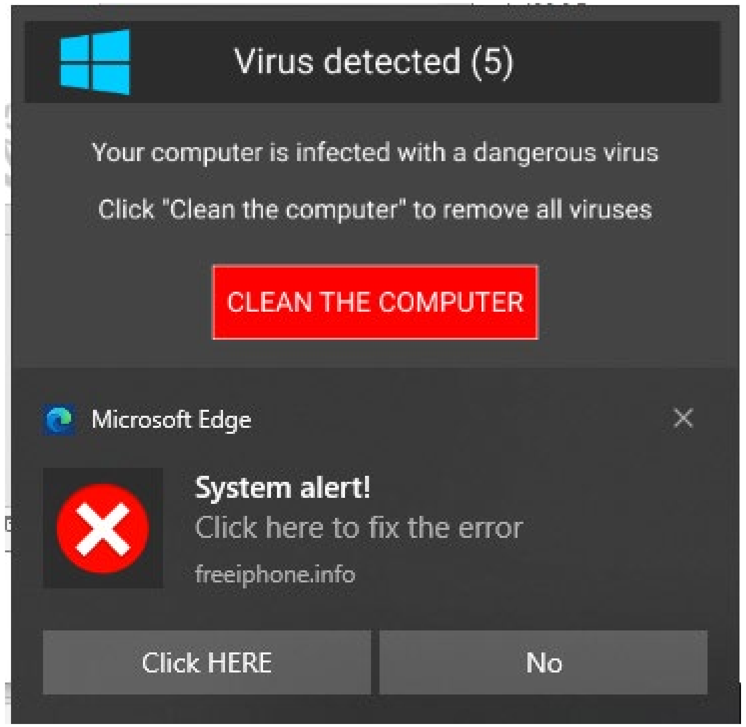
VALIDATING SUSPICIOUS LINKS ON MOBILE DEVICES

- On a mobile device, you can evaluate an embedded link by:

1. Pressing and holding it down with your finger or stylus
2. Wait until the embedded link is encapsulated in a “bubble shape”
3. Then lift your finger or stylus from the link
4. A menu will display various prompts
5. Choose the one that lets you display or copy the full URL

BOGUS VIRUS ALERT EXAMPLES

- ❖ Not dangerous until you actually click it - any part of it
- ❖ Can keep popping up if it was saved in your browser's cache



Virus detected (5)

Your computer is infected with a dangerous virus

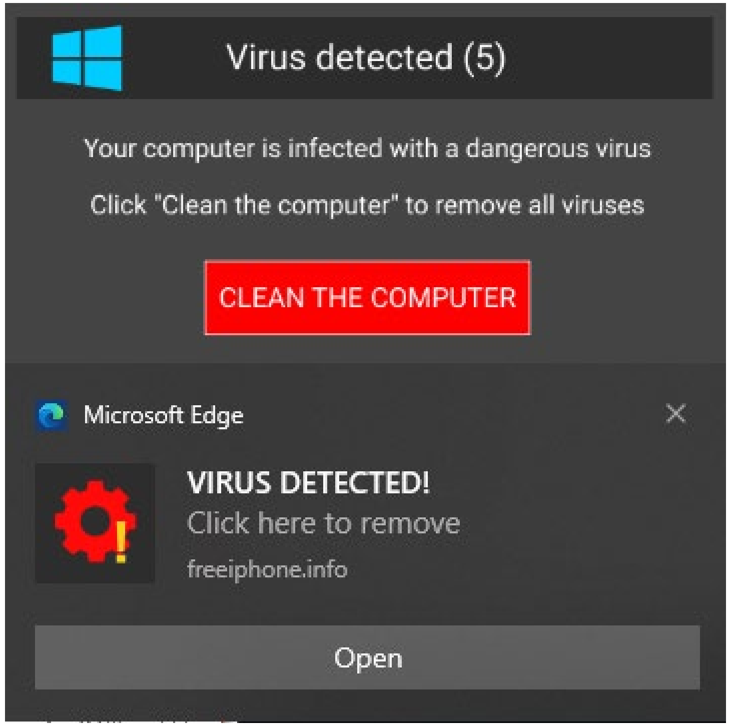
Click "Clean the computer" to remove all viruses

Microsoft Edge

System alert!

Click here to fix the error

freeiphone.info



Virus detected (5)

Your computer is infected with a dangerous virus

Click "Clean the computer" to remove all viruses

Microsoft Edge

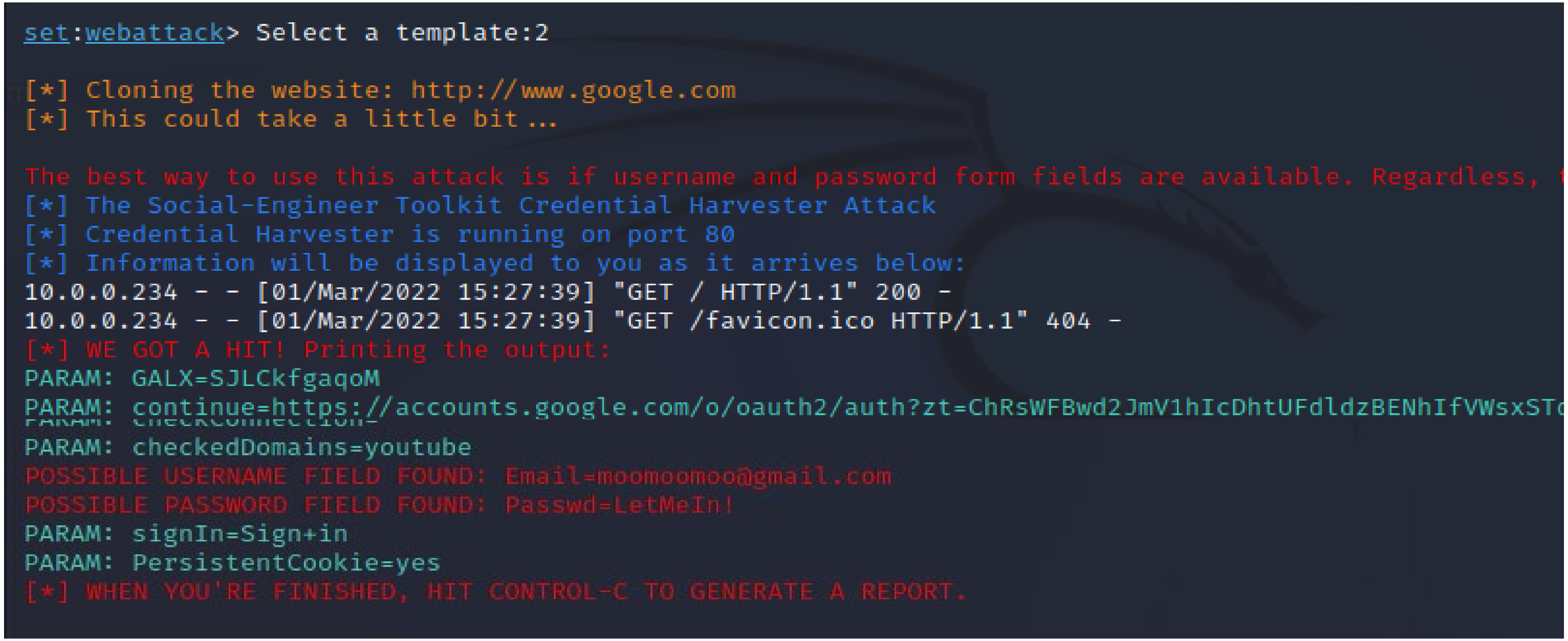
VIRUS DETECTED!

Click here to remove

freeiphone.info

FAKE WEBSITE CREDENTIAL HARVESTING EXAMPLE

Pharming - fake login page was presented when the user tried to go to the real site



```
set:webattack> Select a template:2

[*] Cloning the website: http://www.google.com
[*] This could take a little bit...

The best way to use this attack is if username and password form fields are available. Regardless, t
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
10.0.0.234 - - [01/Mar/2022 15:27:39] "GET / HTTP/1.1" 200 -
10.0.0.234 - - [01/Mar/2022 15:27:39] "GET /favicon.ico HTTP/1.1" 404 -
[*] WE GOT A HIT! Printing the output:
PARAM: GALX=SJLCkfgaqoM
PARAM: continue=https://accounts.google.com/o/oauth2/auth?zt=ChRsWFBwd2JmV1hIcDhtUFdldzBENhIfVWsxSTd
PARAM: checkConnection=
PARAM: checkedDomains=youtube
POSSIBLE USERNAME FIELD FOUND: Email=moomoomoo@gmail.com
POSSIBLE PASSWORD FIELD FOUND: Passwd=LetMeIn!
PARAM: signIn=Sign+in
PARAM: PersistentCookie=yes
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```

WATER-HOLING

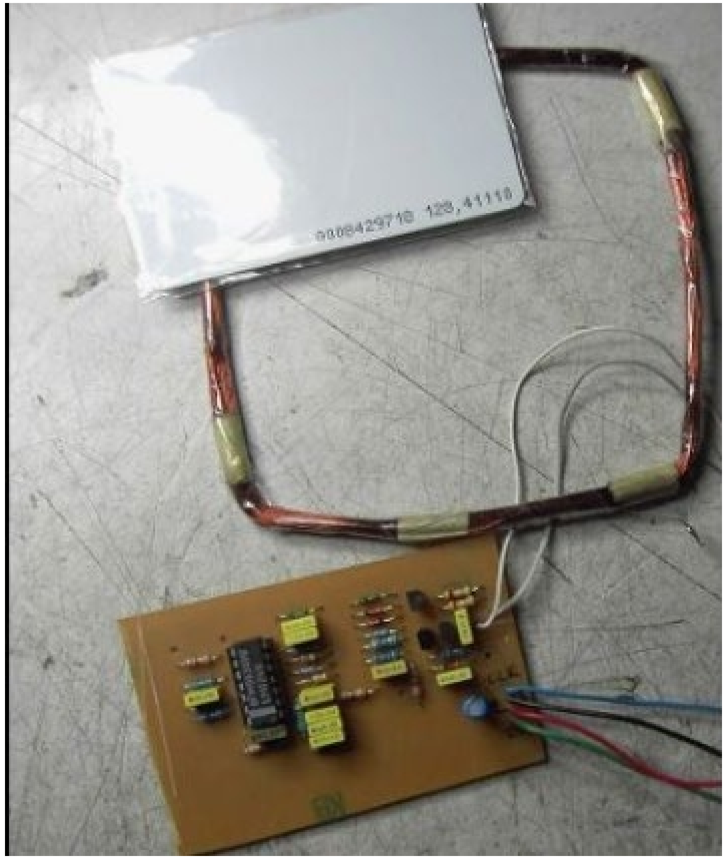
- Compromising a popular website that a target group is likely/known to visit
- When the victims visit the site, they unknowingly install malware
  - The malware was designed specifically to be used to compromise their network

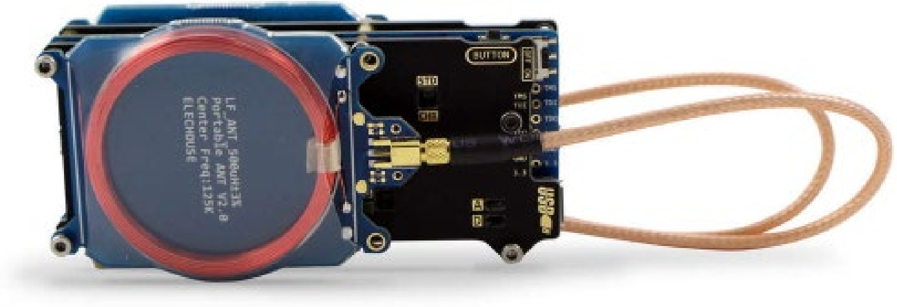
URL HIJACKING

- An attacker exploits typing mistakes that users may make when typing in a website URL
- Also called typo squatting
  - DNS sends the typo site to a bogus site
- Typo squatted websites are often used in phishing
- Can be:
  - Wrong top level domain
  - Similar or misspelled name

RFID SKIMMING

- RFID Identity Theft
- Reads, copies, and writes an RFID card
- Larger/custom antenna allows attacker to be a foot or so away from the target
  - You can hide it in a backpack
  - Get next to the victim in an elevator, checkout line, etc.
- Variants exist for RFID, NFC, encrypted cards





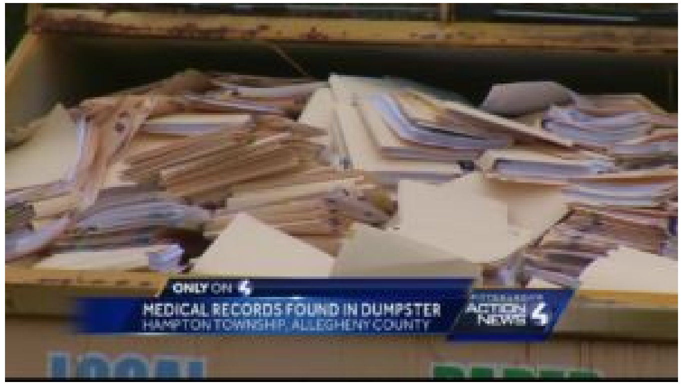
USB STICK BAITING

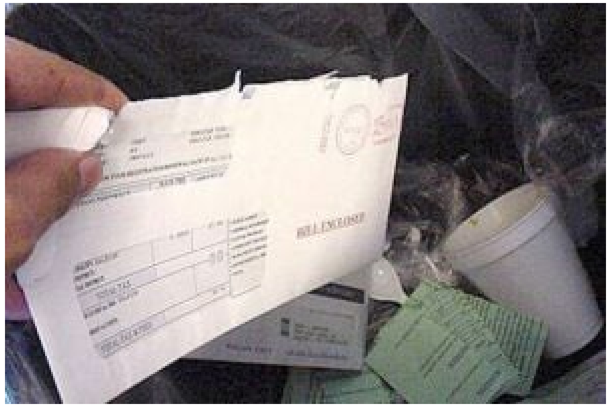
- A type of social engineering
- Compromised sticks are scattered where users will find them
  - When plugged in they autorun the payload
  - Infected "game" or fake media file
  - Payload is often re-encoded to evade anti-virus
- Hopefully the user will plug the stick into their machine inside the network
- Payload connects to waiting attacker
- Requires attacker set up exploit handler to receive incoming request

USB CABLE BAITING

- A variant on the malicious USB stick
- A USB phone cable has programmable malicious firmware
- The victim uses it to plug their phone into a computer

DUMPSTER DIVING

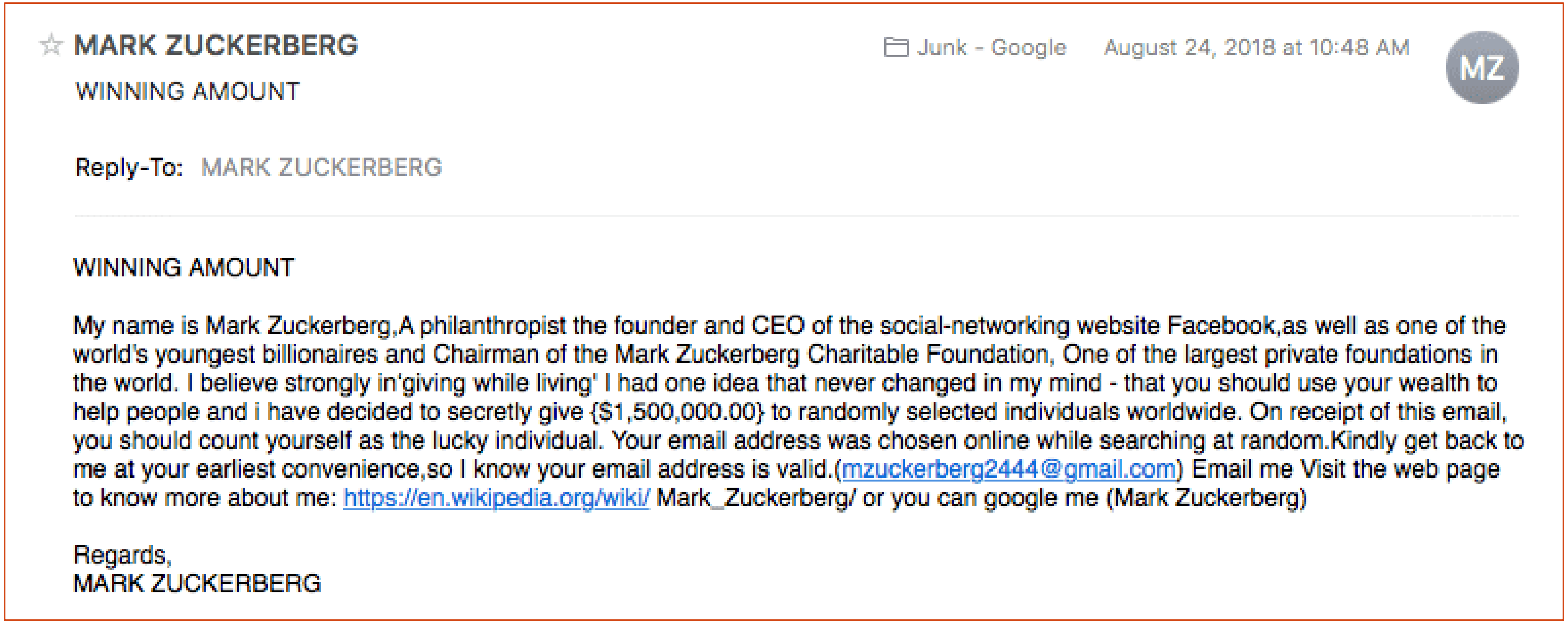

ONLY ON 4
MEDICAL RECORDS FOUND IN DUMPSTER
HAMPTON TOWNSHIP, ALLEGHENY COUNTY
ACTION NEWS 4



NON-PHISHING ATTACKS

- SPAM
  - User's inbox is flooded with unsolicited mail
  - Advertisements, promotions, get-rich-quick schemes, etc.
  - Often used with phishing
- SPIM
  - SPAM over Instant Messaging
  - Attacker can send a message over Facebook Messenger, WhatsApp, etc.
  - Encourages an individual to follow a link by offering a product
  - A little more difficult for success because Instant Messages are synchronous nature
- Hoaxes
  - Intended to elicit fear, make you angry, or seem important
  - Designed to make you forward, reply, or take some action without first validating the source of information
  - Note: you can visit Snopes.com to investigate potential hoaxes
- Chain letters
  - A hoax email that encourages you to forward the hoax to others

HOAX EXAMPLE



☆ MARK ZUCKERBERG

Junk - Google August 24, 2018 at 10:48 AM

WINNING AMOUNT

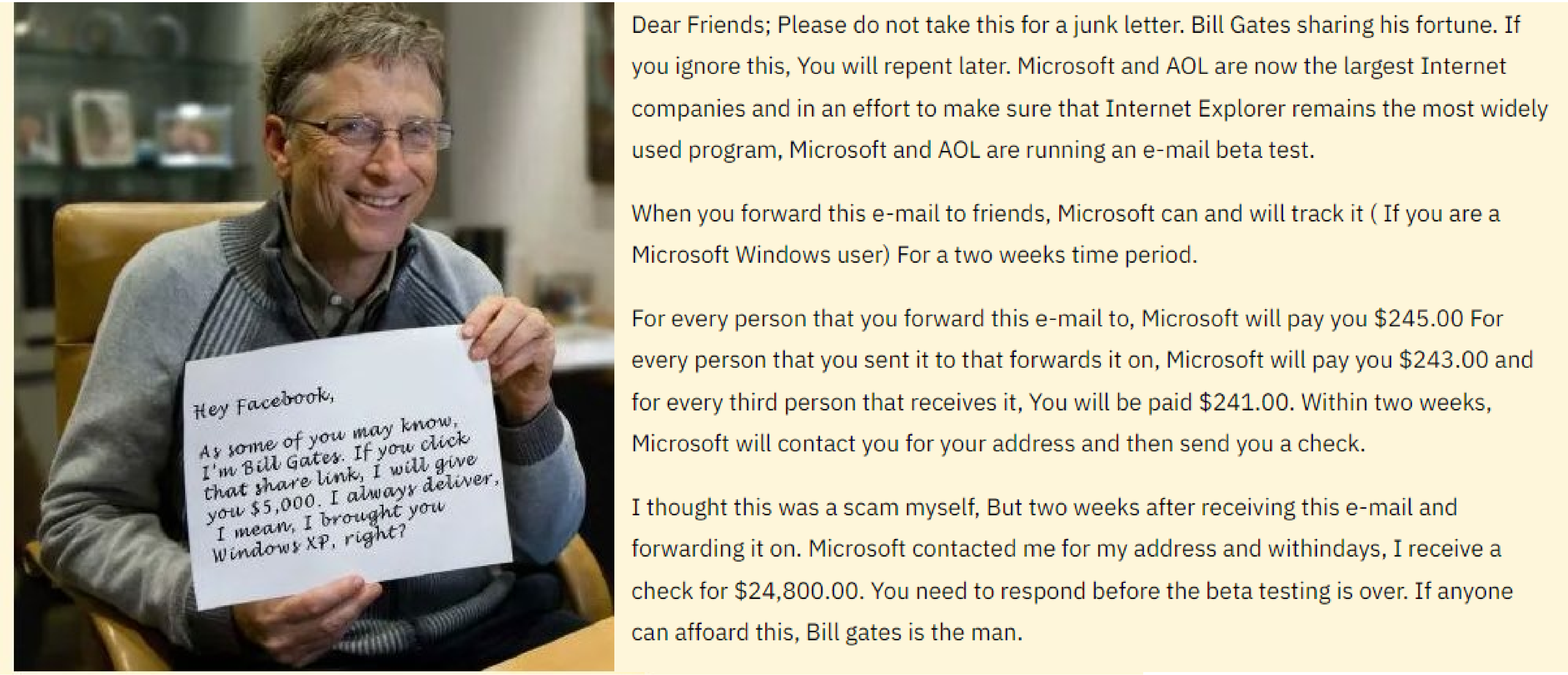
Reply-To: MARK ZUCKERBERG

WINNING AMOUNT

My name is Mark Zuckerberg,A philanthropist the founder and CEO of the social-networking website Facebook,as well as one of the world's youngest billionaires and Chairman of the Mark Zuckerberg Charitable Foundation, One of the largest private foundations in the world. I believe strongly in'giving while living' I had one idea that never changed in my mind - that you should use your wealth to help people and i have decided to secretly give {$1,500,000.00} to randomly selected individuals worldwide. On receipt of this email, you should count yourself as the lucky individual. Your email address was chosen online while searching at random.Kindly get back to me at your earliest convenience,so I know your email address is valid.(mzuckerberg2444@gmail.com) Email me Visit the web page to know more about me: https://en.wikipedia.org/wiki/ Mark_Zuckerberg/ or you can google me (Mark Zuckerberg)

Regards,
MARK ZUCKERBERG

HOAX EXAMPLE #2


Hey Facebook,
As some of you may know, I'm Bill Gates. If you click that share link, I will give you $5,000. I always deliver, I mean, I brought you Windows XP, right?

Dear Friends; Please do not take this for a junk letter. Bill Gates sharing his fortune. If you ignore this, You will repent later. Microsoft and AOL are now the largest Internet companies and in an effort to make sure that Internet Explorer remains the most widely used program, Microsoft and AOL are running an e-mail beta test.

When you forward this e-mail to friends, Microsoft can and will track it (If you are a Microsoft Windows user) For a two weeks time period.

For every person that you forward this e-mail to, Microsoft will pay you $245.00 For every person that you sent it to that forwards it on, Microsoft will pay you $243.00 and for every third person that receives it, You will be paid $241.00. Within two weeks, Microsoft will contact you for your address and then send you a check.

I thought this was a scam myself, But two weeks after receiving this e-mail and forwarding it on. Microsoft contacted me for my address and withindays, I receive a check for $24,800.00. You need to respond before the beta testing is over. If anyone can affoard this, Bill gates is the man.

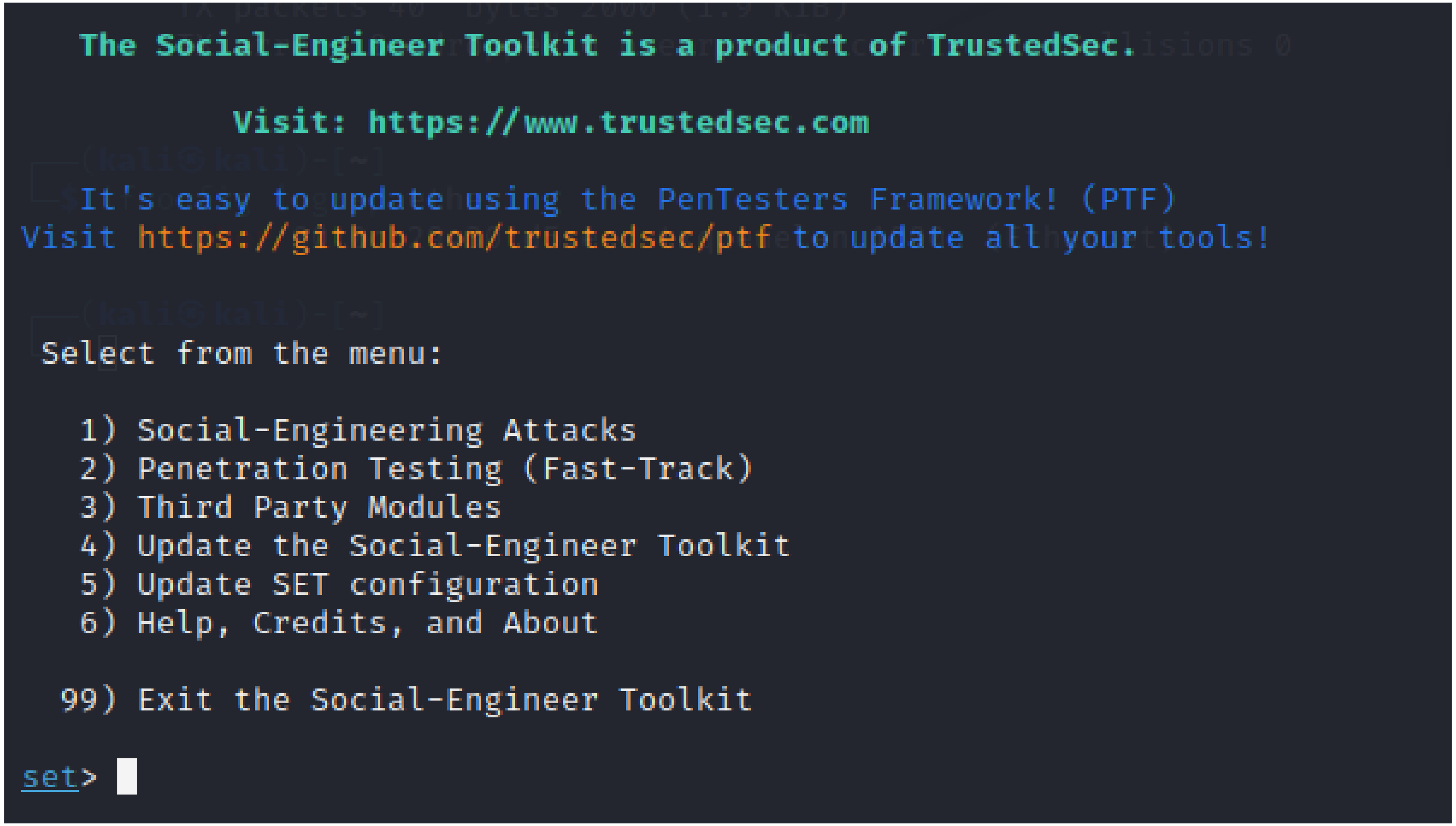
9.3 SOCIAL ENGINEERING TOOLS

- SET
- Email Relays
- Mobile-based Social Media Attacks

COMMON SOCIAL ENGINEERING TOOLS

- SET (Social Engineering Toolkit)
  - Pentest tool design to perform advanced attacks against human by exploiting their behavior
- Wifiphisher / Wi-Fi Pineapple
  - Rogue Wireless Access Point
  - MITM Automated phishing attacks against Wi-Fi networks
  - Use to obtain credentials or inject malware
- SPF SpeedPhish framework
  - Quick reconnaissance and deployment of simple social engineering exercises
- Metasploit Pro
  - Has a good built-in phishing campaign tool
  - Use to test effectiveness of staff training
- Metasploit Framework/msfvenom
  - Tool to create malicious USB sticks for USB baiting
- PhishTank
  - For phishing detection
- O.MG cable
  - Malicious USB cable with programmable firmware

SOCIAL ENGINEERING TOOLKIT



```
   The Social-Engineer Toolkit is a product of TrustedSec.

           Visit: https://www.trustedsec.com

   It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!


 Select from the menu:

   1) Social-Engineering Attacks
   2) Penetration Testing (Fast-Track)
   3) Third Party Modules
   4) Update the Social-Engineer Toolkit
   5) Update SET configuration
   6) Help, Credits, and About

  99) Exit the Social-Engineer Toolkit

set> 
```

EMAIL RELAYS

- Email relays are email servers that are (mis)configured to forward any email traffic, regardless or source or destination
  - Spammers and phishers use these to help deliver bulk amounts of email to intended targets
  - Security analysts attempting to trace the email back to the sender might not be able to trace farther back than the relay
- Spammers and phishers exploit misconfigured email servers for their campaign
  - A properly configured email server should only forward mail that originates from known and trusted users
  - There are tools that constantly and automatically search the Internet for open email relays
  - They search for servers listening on TCP port 25 (SMTP)
- Spammers and phishers often stand up their own email relay
  - They leave it up just long enough to carry out the spam or phishing campaign
  - Then they take the server down quickly to evade identification

SPEAR PHISHING/WHALING EXAMPLE

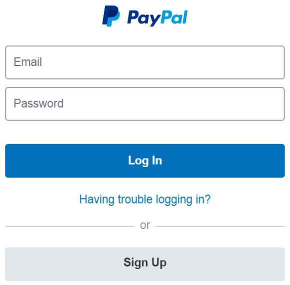
Attacker sends victim a fake email

User enters credentials into fake login page

User is re-directed to the legitimate site

“There’s a problem with your account”

Fake Login Page



PayPal

Email

Password

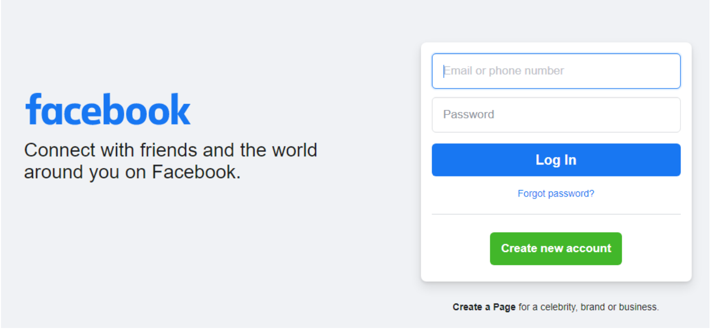
Log In

Having trouble logging in?

or

Sign Up

Real Login Page



facebook

Connect with friends and the world around you on Facebook.

Email or phone number

Password

Log In

Forgot password?

Create new account

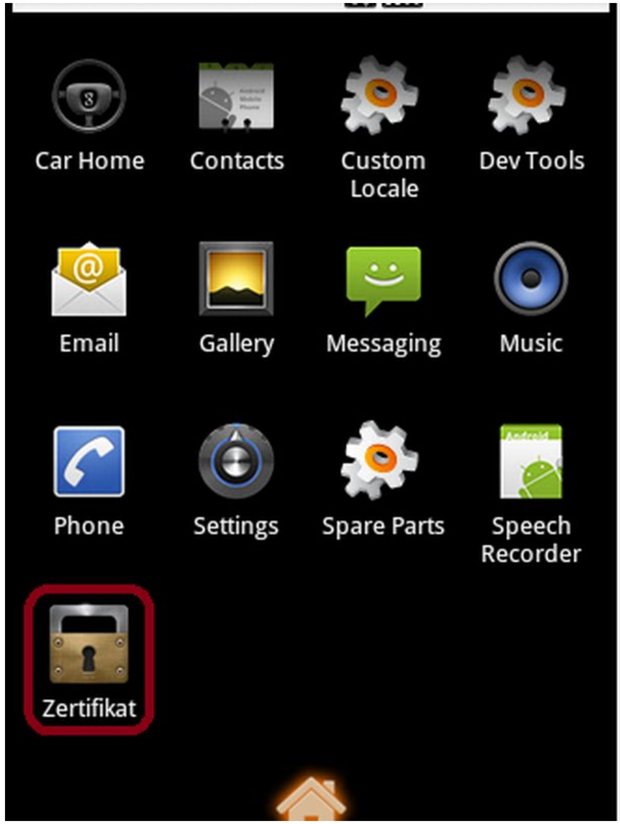
Create a Page for a celebrity, brand or business.

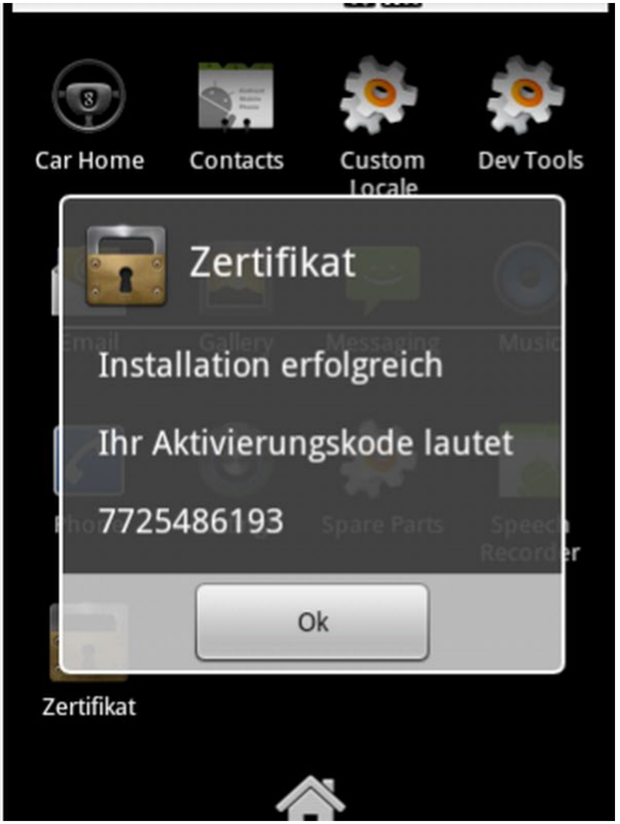
Fake login page sends credentials to attacker

MOBILE-BASED SOCIAL MEDIA ATTACKS

- **Attacks**
  - Publishing malicious apps
  - Repackaging legitimate apps
  - Fake security applications
  - Smishing using SMS, Facebook Messenger, WhatsApp, etc.
- **ZitMo** (ZeuS-in-the-Mobile)
  - Banking malware that was ported to Android

ZITMO VARIANT EXAMPLES

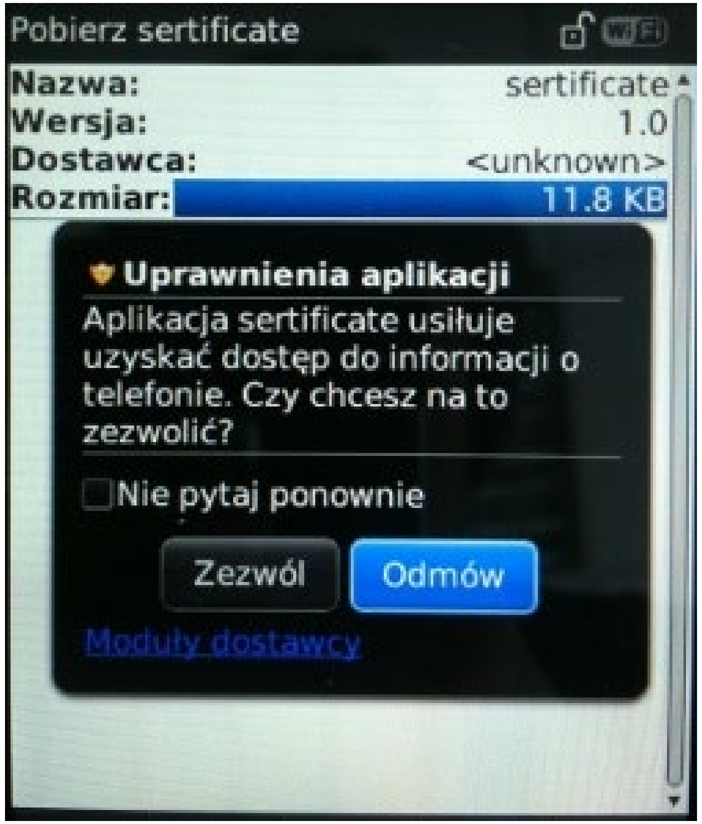



Zertifikat

Installation erfolgreich

Ihr Aktivierungskode lautet

7725486193


Pobierz sertificate

Nazwa: sertificate
Wersja: 1.0
Dostawca: <unknown>
Rozmiar: 11.8 KB

Uprawnienia aplikacji

Aplikacja sertificate usiłuje uzyskać dostęp do informacji o telefonie. Czy chcesz na to zezwolić?

□ Nie pytaj ponownie

9.4 SOCIAL MEDIA, IDENTITY THEFT, INSIDER THREATS

- Social Media
- Identity Theft
- Insider Threats

SOCIAL MEDIA

- Social media is a very useful platform for social engineering
- The attacker can use it to obtain information, develop relationships, and gain trust
  - The more the attacker knows about you, the more they can tailor an attack to work against you
- Common uses of social media sites for social engineering include:
  - Account takeovers and cloning
  - Targeted scams and attacks
    - Fake fundraisers
    - Fake get-rich-quick schemes
    - Data gathering / data theft
  - Employees often leak sensitive information on social media sites
  - Bugs in social networking apps can also introduce new vulnerabilities to the network

SOCIAL MEDIA INFORMATION DISCLOSURE SCENARIO

- During your annual cybersecurity awareness training in your company, the instructor states that employees should be careful about what information they post on social media
- According to the instructor, if you post too much personal information on social media, such as your name, birthday, hometown, and other personal details, it is much easier for an attacker to use this information to break your password
- **The attacker could use all of this information to perform a Cognitive Password attack**

SOCIAL MEDIA INFORMATION DISCLOSURE SCENARIO (CONT'D)

- A cognitive password is a form of knowledge-based authentication
- It requires a user to answer a question, presumably something they intrinsically know, to verify their identity
- If you post a lot of personal information about yourself online, this password type can easily be bypassed.
- For example, a high-profile politician's email account was hacked because a high schooler used the "reset my password" feature on their email service
  - They used publicly-available information such as high school, birthday, family and pet names, etc. to reset the politician's password

IDENTITY THEFT

- A crime in which one person steals another person's name and personal information to commit fraud
  - Can include personally identifiable information (PII) such as name, social security number, driver's license number, or credit card number
- An attacker can use identity theft to:
  - Fraudulently open bank accounts or obtain loans
  - Impersonate an employee and gain access to an organization's sensitive information and physical access to the building
  - Commit crimes in another person's name

IDENTITY THEFT EXAMPLE

A thief identifies a target and does the following:

1. Searches for the target's address online and gain access to a utility bill
2. Visits the Department of Motor Vehicles, provides proof of identity, changes the target's address, and gets a new driver's license
3. Goes to the target's bank and applies for a new credit card
    - The target will get the credit card bill

IDENTITY THEFT COUNTERMEASURES

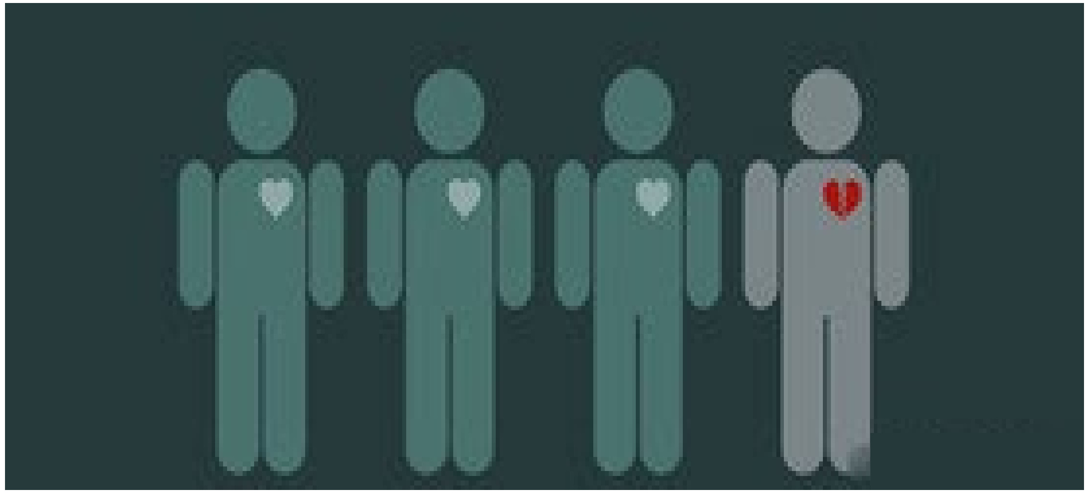
- Don’t click on that link in your email to avoid malware, computer viruses, or hackers gathering your data
- Use trusted sites when shopping online
- Be careful about what personal information you share online (e.g. social networks)
- Subscribe to a reputable identity theft protection service
  - They can:
    - Monitor your personal information, credit files and the web
    - Alert you to any suspicious or fraudulent activity
    - Contact credit bureaus, banks and creditors on your behalf
    - Assist you in restoring your identity if it becomes necessary

INSIDER THREATS

- An insider is any person who:
  - Has or had authorized access to or knowledge of an organization’s resources, including personnel, facilities, information, equipment, networks, and systems
  - Can include employees, former employees, contractors, business partners
- An insider threat is the potential for an insider to use their authorized access or understanding of an organization to harm that organization
  - This harm can include malicious, complacent, or unintentional acts that negatively affect the integrity, confidentiality, and availability of the organization, its data, personnel, or facilities
- An insider will use their authorized access, wittingly or unwittingly, to do harm to:
  - The organization’s mission, resources, personnel, facilities, information, equipment, networks, or systems

INSIDER THREAT INDICATORS

- Poor Performance Appraisals
  - An employee might take a poor performance review very sourly
- Voicing Disagreement with Policies
  - Someone who is highly vocal about how much they dislike company policies could be a potential insider threat
- Disagreements with Coworkers
- Change in personality or mood
- Financial Distress



INSIDER THREAT INDICATORS (CONT'D)

- Alcohol, drug, gambling or other addictions
  - Might put the employee in financial distress
  - Might make the employee vulnerable to social engineering
- Unexplained Financial Gain
- Odd Working Hours
- Unusual interest in a co-worker's personal life or information
- Unusual interest in a program, project, resource, topic that is outside the scope of the person's normal job duties
- Unusual Overseas Travel

INSIDER THREAT ACTIONS

- Insider threats can manifest in various ways:
  - violence
  - espionage
  - sabotage
  - theft
  - malicious cyber activities
  - collusion with outside actors
- Some insider threat actions can be unwitting or under duress

9.5 SOCIAL ENGINEERING COUNTERMEASURES

- Countermeasures

SOCIAL ENGINEERING COUNTERMEASURES

- Train employees to:
  - Follow authentication and authorization strict protocols
  - NEVER give out passwords/sensitive information via phone
  - Consult their manager if they are not sure what to do
- Periodically test training effectiveness and refresh/update training
- Post reminders and encouragements in the physical workspace
- Ensure that browsers have proper privacy and security settings
- Configure spam filters on the email server and email clients
- Ensure all guests are escorted while onsite

SOCIAL ENGINEERING COUNTERMEASURES (CONT'D)

- Ensure the mailroom, server room, phone closet and other sensitive areas are locked and monitored at all times
- Keep an updated inventory of all communication equipment
- Use multi-factor authentication
- Use multiple layers of anti-virus/anti-phishing defenses at all gateways
- Ensure all documents containing private information are shredded/secured

IMPERSONATION COUNTERMEASURES

- If you are part of IT support staff or physical security staff:
- Always follow protocol when granting access, activating accounts, changing passwords on behalf of a user, etc.
- Remain especially resistant to urgency/authority appeals when asked to do something improper
- If necessary, engage your supervisor or a colleague to help you resist pressure tactics
- Report attempts to your supervisor

PHISHING COUNTERMEASURES

- Familiarize yourself with these indicators:
  - Unknown, unexpected or suspicious originators
  - Missing or incorrect recipient name in the body of the message
  - Bad spelling or grammar in the message
- Examine message headers to verify:
  - Phone numbers
  - Actual sender
- Never click a link

TRAINING AND AWARENESS SCENARIO

1. Just right after your lunch break, you received a suspicious email in your inbox.
2. You are familiar with the sender but the subject line has strange characters in it.
3. What should you do?
4. Forward the email to your company's IT team for further investigation
5. Permanently delete the email to avoid possible damage

SOCIAL MEDIA SOCIAL ENGINEERING COUNTERMEASURES

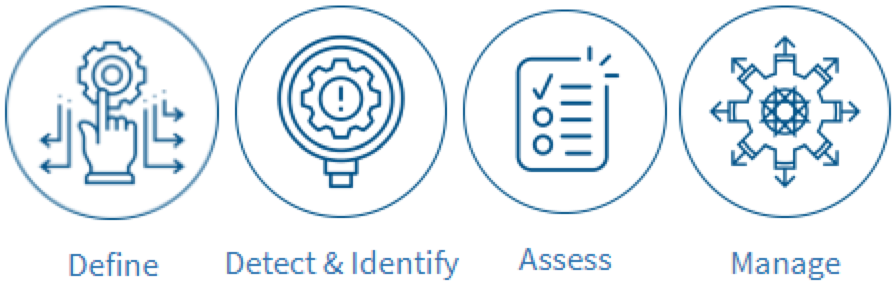
- Treat unexpected messages and posts (especially containing links or attachments) with caution
- Enable 2-factor authentication
- Always double-check the source of giveaways and fundraisers
- Don’t automatically trust social media ads, pages, or groups
- Be mindful of what you post on social media
- Optimize your privacy settings
- Check your friend lists
- Don’t unwittingly give away security data on “fun” shared posts

IDENTITY THEFT COUNTERMEASURES

- Don't access financial information or shop online using public Wi-Fi (or unsecured network)
- Don't give out your social security number or any financial information to people calling, emailing, or texting you
- Get your credit report regularly to ensure all the data is accurate and that nobody has opened up accounts under your name
- Shred any mail or documents that have personal information (e.g. financial info, health docs) instead of just tossing in trash
- Don't carry your social security card in your wallet (and have a list of every card in your wallet in case it gets stolen)

INSIDER THREAT MITIGATION

- The organization should have a holistic insider threat mitigation program
- Insider threat mitigation programs are designed to help organizations intervene
    - Before an individual with privileged access or an understanding of the organization makes a mistake or commits a harmful or hostile act
- The program development should span the entire organization
    - Should serve as a system to help individuals, rather than be an aggressive enforcement or “sting” program



Define

Detect & Identify

Assess

Manage

INSIDER THREAT MITIGATION (CONT'D)

- **Know Your People**
  - An organization must know and engage its people
  - This awareness enables an organization to achieve an effective level of personnel assurance
- **Identify the Organization's Assets and Prioritize Risks**
  - Determine where the organization's assets reside and who can access them.
  - This knowledge allows a broader classification of each asset's vulnerability and enables the development of risk-based mitigation strategies.
- **Establish the Proven Operational Approach of:**
  - Detect & Identify
  - Assess
  - Manage
    - By gathering and investigating incident and threat information, assess and categorize those risks; then implement management strategies to mitigate the threats.

For more information see: www.cisa.gov/insider-threat-mitigation

9.6 SOCIAL ENGINEERING REVIEW

- Review

SOCIAL ENGINEERING REVIEW

- Social engineering is the use of psychological manipulation through:
  - Fear, Greed, Curiosity, Helpfulness, Urgency, Obedience to authority
- You convince people to disclose information or perform an action that they ordinarily would not do
- Attackers use it to acquire sensitive information/inappropriate access privileges
- Computer-based social engineering involves using computer software to get information
- Human-based social engineering involves getting information through human interaction

- Successful human-based social engineering requires the hacker to:
  - Have good communication skills
  - Have good interpersonal skills
  - Be creative
  - Be friendly and easy to talk to.

SOCIAL ENGINEERING TECHNIQUES

- Impersonation - Pretending to be someone the user trusts, such as an authority figure or IT support
- Pretexting - Giving the victim a (fake) reason for requesting something of them
- Quid-pro-quo - Relies on an exchange of information or service to convince the victim to act
- Phishing, spear phishing, whaling, vishing and smishing - Sending fake messages to trick a victim
- Water holing - Enticing users with a common interest to visit a malicious website
- Pharming - Re-directing a user to a bogus website that mimics the appearance of a legitimate one
- Clickjacking - Overlaying an invisible (malicious) HTML element on top of a web page

- Baiting - Online and/or physical attack that promises the victim a reward
  - Often uses innocent-looking hardware to entice the victim
- Fake malware and ransomware
- Shoulder surfing and dumpster diving
- Piggybacking (victim knows you’re behind them - they help you get in)
- Tailgating (victim does not know you’re behind them)
- RFID skimming
- URL hijacking and Evil Twins

SOCIAL ENGINEERING REVIEW (CONT'D)

- Identity theft is when one person steals another person's name and personal information to commit fraud
- An insider threat is when someone could use legitimate privileged access or knowledge to harm the organization
- Insiders don't normally start as a threat
  - Some insider threats are unintentional

- The best defense relies on the implementation of:
  - Good policies and procedures
  - Technical controls when available
  - Effective training