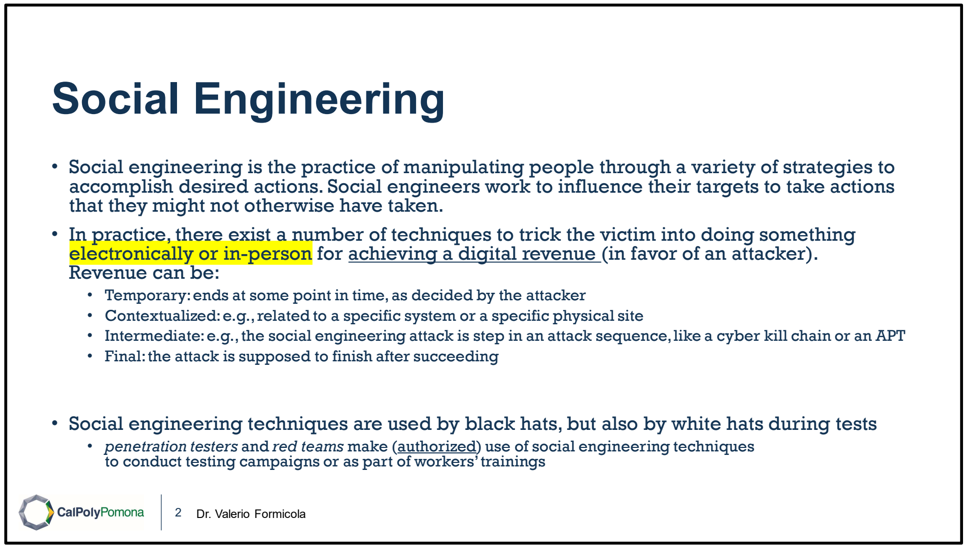
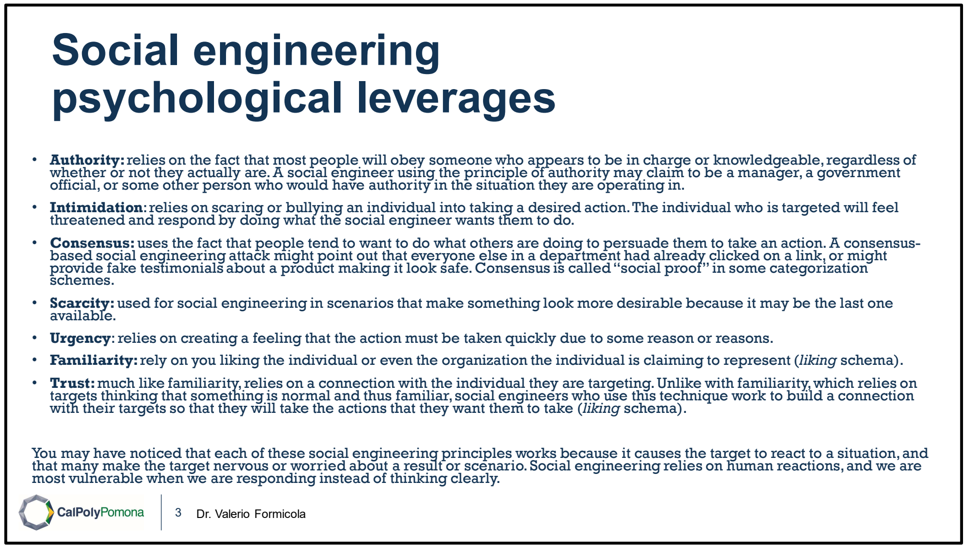
Social Engineering



Social Engineering

- Social engineering is the practice of manipulating people through a variety of strategies to accomplish desired actions. Social engineers work to influence their targets to take actions that they might not otherwise have taken.
- In practice, there exist a number of techniques to trick the victim into doing something electronically or in-person for achieving a digital revenue (in favor of an attacker). Revenue can be:
  - Temporary: ends at some point in time, as decided by the attacker
  - Contextualized: e.g., related to a specific system or a specific physical site
  - Intermediate: e.g., the social engineering attack is step in an attack sequence, like a cyber kill chain or an APT
  - Final: the attack is supposed to finish after succeeding
- Social engineering techniques are used by black hats, but also by white hats during tests
  - *penetration testers* and *red teams* make (authorized) use of social engineering techniques to conduct testing campaigns or as part of workers' trainings



Social engineering psychological leverages

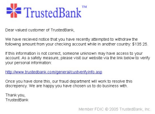
- **Authority:** relies on the fact that most people will obey someone who appears to be in charge or knowledgeable, regardless of whether or not they actually are. A social engineer using the principle of authority may claim to be a manager, a government official, or some other person who would have authority in the situation they are operating in.
- **Intimidation**: relies on scaring or bullying an individual into taking a desired action. The individual who is targeted will feel threatened and respond by doing what the social engineer wants them to do.
- **Consensus:** uses the fact that people tend to want to do what others are doing to persuade them to take an action. A consensus-based social engineering attack might point out that everyone else in a department had already clicked on a link, or might provide fake testimonials about a product making it look safe. Consensus is called "social proof" in some categorization schemes.
- **Scarcity:** used for social engineering in scenarios that make something look more desirable because it may be the last one available.
- **Urgency**: relies on creating a feeling that the action must be taken quickly due to some reason or reasons.
- **Familiarity:** rely on you liking the individual or even the organization the individual is claiming to represent (*liking* schema).
- **Trust:** much like familiarity, relies on a connection with the individual they are targeting. Unlike with familiarity, which relies on targets thinking that something is normal and thus familiar, social engineers who use this technique work to build a connection with their targets so that they will take the actions that they want them to take (*liking* schema).

You may have noticed that each of these social engineering principles works because it causes the target to react to a situation, and that many make the target nervous or worried about a result or scenario. Social engineering relies on human reactions, and we are most vulnerable when we are responding instead of thinking clearly.

CalPolyPomona | 3 Dr. Valerio Formicola

Many, if not most, social engineering efforts in the real world combine multiple principles into a single attack. If a penetration tester calls claiming to be a senior leader's assistant in another part of your company (thus leading authority and possibly familiarity responses) and then insists that that senior leader has an urgent need (urgency) and informs their target that they could lose their job if they don't do something immediately (intimidation), they are more likely to be successful in many cases than if they only used one principle. A key part of social engineering is understanding the target, how humans react, and how stress reactions can be leveraged to meet a goal.

Digital Techniques: Phishing



TrustedBank™

Dear valued customer of TrustedBank,

We have recieved notice that you have recently attempted to withdraw the following amount from your checking account while in another country: $135.25.

If this information is not correct, someone unknown may have access to your account. As a safety measure, please visit our website via the link below to verify your personal information:

http://www.trustedbank.com/general/custverifyinfo.asp

Once you have done this, our fraud department will work to resolve this discrepency. We are happy you have chosen us to do business with.

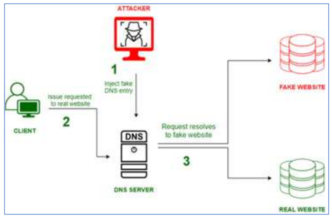
Thank you,
TrustedBank

Member FDIC © 2005 TrustedBank, Inc.

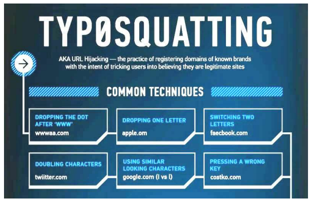
- *Phishing* is a broad term used to describe the fraudulent acquisition of information, often focused on credentials like usernames and passwords, as well as sensitive personal information like credit card numbers and related data.
- Phishing is most often done via **email**, but a wide range of phishing techniques exist, including things like *smishing*, which is phishing via **SMS (text) messages**, and *vishing*, or phishing via **telephone**.
- Specific terms are also used for specific targets of phishing attempts.
  - *Spear phishing* targets specific individuals or groups in an organization in an attempt to gather desired information or access.
  - *Whaling*, much like spear phishing, targets specific people, but whaling is aimed at senior employees like CEOs and CFOs—"big fish" in the company, thus the term whaling.
- Like most social engineering techniques, one of the most common defenses against phishing of all types is awareness.
  - Teaching staff members about phishing and how to recognize and respond to phishing attacks, and even staging periodic exercises, are all common means of decreasing the risk of successful phishing attacks.
- Technical means also exist, including filtering that helps prevent phishing using reputation tools, keyword and text pattern matching, and other technical methods of detecting likely phishing emails, calls, or texts.

Digital Techniques: WebSite attacks

- *Pharming* is one example of website attack in social engineering: Pharming attacks redirect traffic away from legitimate websites to malicious versions. Pharming typically requires a successful technical attack that can change DNS entries on a local PC or on a trusted local DNS server, allowing the traffic to be re-directed.
- *Typo squatters* use misspelt and slightly off but similar to the legitimate site URLs to conduct typosquatting attacks: Typo squatters rely on the fact that people will mistype URLs and end up on their sites, thus driving ad traffic or even sometimes using the typo-based website to drive sales of similar but not legitimate products.
- *Watering hole attacks* don't redirect users (unlike pharming); instead, they use websites that target frequent to attack them. These frequently visited sites act like a watering hole for animals and allow the attackers to stage an attack, knowing that the victims will visit the site. Once they know what site their targets will use, attackers can focus on compromising it, either by targeting the site or deploying malware through other means such as an advertising network (malvertising).

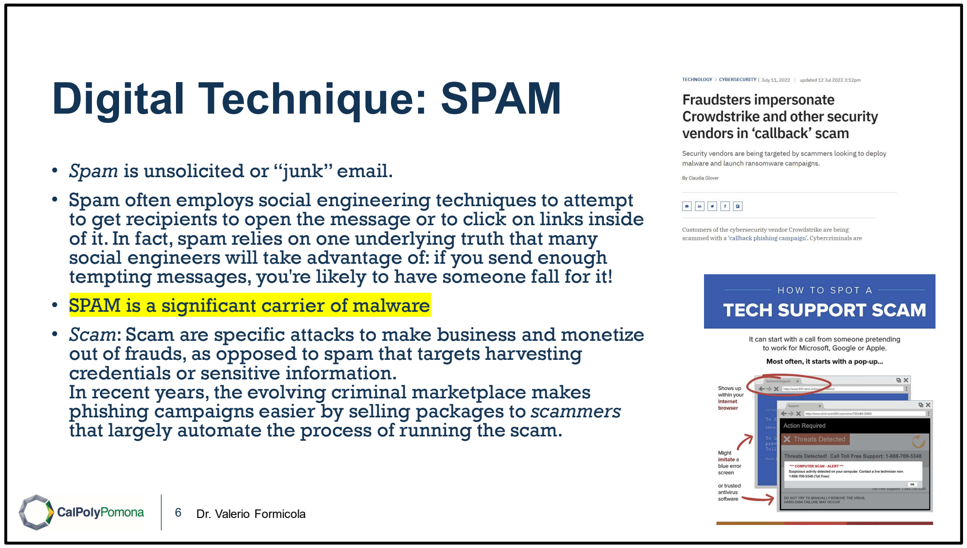


Pharming attack



TYPØSQUATTING

AKA URL Hijacking — the practice of registering domains of known brands with the intent of tricking users into believing they are legitimate sites



Digital Technique: SPAM

- *Spam* is unsolicited or "junk" email.
- Spam often employs social engineering techniques to attempt to get recipients to open the message or to click on links inside of it. In fact, spam relies on one underlying truth that many social engineers will take advantage of: if you send enough tempting messages, you're likely to have someone fall for it!
- SPAM is a significant carrier of malware
- *Scam*: Scam are specific attacks to make business and monetize out of frauds, as opposed to spam that targets harvesting credentials or sensitive information.
  In recent years, the evolving criminal marketplace makes phishing campaigns easier by selling packages to *scammers* that largely automate the process of running the scam.

TECHNOLOGY > CYBERSECURITY | July 11, 2022 | updated 12 Jul 2022 3:12pm

Fraudsters impersonate Crowdstrike and other security vendors in 'callback' scam

Security vendors are being targeted by scammers looking to deploy malware and launch ransomware campaigns.

By Claudia Glover

Customers of the cybersecurity vendor Crowdstrike are being scammed with a 'callback phishing campaign'. Cybercriminals are

HOW TO SPOT A

TECH SUPPORT SCAM

It can start with a call from someone pretending to work for Microsoft, Google or Apple.

Most often, it starts with a pop-up...

Shows up within your internet browser
Might imitate a blue error screen
or trusted antivirus software
Technical Support
http://www.917-alert.online/.../detect
Support
http://www.alert.scan001.com/error730a84-0983
Action Required
Threats Detected
Threats Detected! Call Toll Free Support: 1-888-709-5348
*** COMPUTER SCAN - ALERT ***
Suspicious activity detected on your computer. Contact a live technician now. 1-888-709-5348 (Toll Free)
OK
DO NOT TRY TO MANUALLY REMOVE THE VIRUS, HARD-DISK FAILURE MAY OCCUR

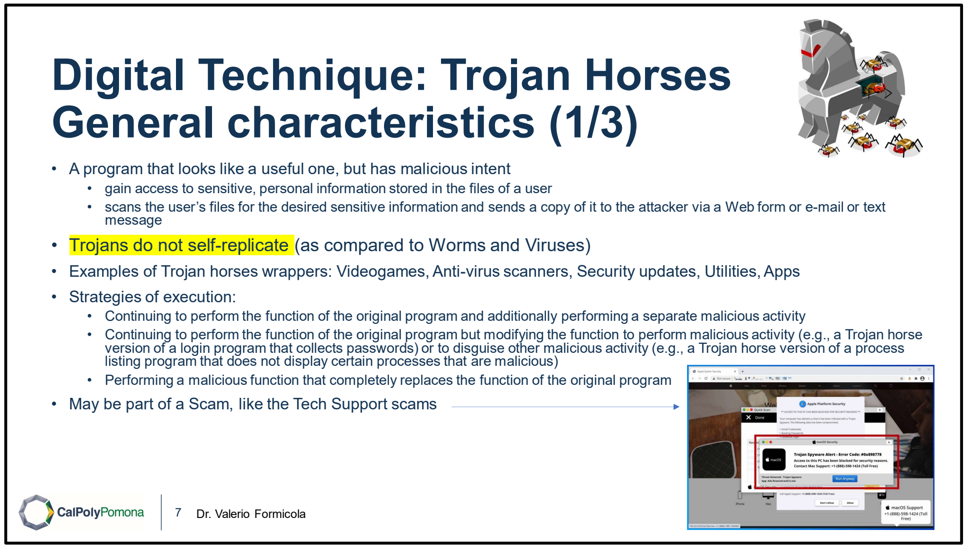
CalPolyPomona | 6 Dr. Valerio Formicola

With the explosive growth of the Internet over the last few decades, the widespread use of e-mail, and the extremely low cost required to send large volumes of e-mail, has come the rise of unsolicited bulk e-mail, commonly known as spam. [SYMA16] notes that more than half of inbound business e-mail traffic is still spam, despite a gradual decline in recent years. This imposes significant costs on both the network infrastructure needed to relay this traffic, and on users who need to filter their legitimate e-mails out of this flood. In response to this explosive growth, there has been the equally rapid growth of the anti-spam industry that provides products to detect and filter spam e-mails. This has led to an arms race between the spammers devising techniques to sneak their content through, and with the defenders, efforts to block them [KREI09].

However, the spam problem continues, as spammers exploit other means of reaching their victims. This includes the use of social media, reflecting the rapid growth in the use of these networks. For example, [SYMA16] described a successful weightloss spam campaign that exploited hundreds of thousands of fake Twitter accounts, mutually supporting and reinforcing each other, to increase their credibility and likelihood of users following them, and then falling for the scam. Social network scams often rely on victims sharing the scam, or on fake offers with incentives, to assist their spread.

While some spam e-mail is sent from legitimate mail servers using stolen user credentials, most recent spam is sent by botnets using compromised user systems, as we will discuss in Section 6.6. A significant portion of spam e-mail content is just advertising, trying to convince the recipient to purchase some product online, such as pharmaceuticals, or used in scams, such as stock, romance or fake trader scams, or money mule job ads. But spam is also a significant carrier of malware. The e-mail may have an attached document, which, if opened, may exploit a software vulnerability to install malware on the user's system, as we discussed in the previous section. Or, it may have an attached Trojan horse program or scripting code that, if run, also installs malware on the user's system. Some Trojans avoid the need for user agreement by exploiting a software vulnerability in order to install themselves, as we will discuss next. Finally, the spam may be used in a phishing attack, typically directing the user either to a fake website that mirrors some legitimate service, such as an online banking site, where it attempts to capture the user's login and password details; or to complete some form with sufficient personal details to allow the attacker to impersonate the user in an identity theft. In recent years, the evolving criminal marketplace makes phishing campaigns easier by selling packages to scammers that largely automate the process of running the scam [SYMA16]. All of these uses make spam e-mails a significant security concern. However, in many cases, it requires the user's active choice to view the e-mail and any attached document, or to permit the installation of some program, in order for the compromise to occur. Hence the importance of providing appropriate security awareness training to users, so they are better able to recognize and respond appropriately to such e-mails, as we will discuss in Chapter 17.

Tech Support Scams are a growing social engineering concern. These involve call centers calling users about nonexistent problems on their computer systems. If the users respond, the attackers try to sell them bogus tech support or ask them to install Trojan malware or other unwanted applications on their systems, all while claiming this will fix their problem [SYMA16].



Digital Technique: Trojan Horses General characteristics (1/3)

- A program that looks like a useful one, but has malicious intent
  - gain access to sensitive, personal information stored in the files of a user
  - scans the user's files for the desired sensitive information and sends a copy of it to the attacker via a Web form or e-mail or text message
- Trojans do not self-replicate (as compared to Worms and Viruses)
- Examples of Trojan horses wrappers: Videogames, Anti-virus scanners, Security updates, Utilities, Apps
- Strategies of execution:
  - Continuing to perform the function of the original program and additionally performing a separate malicious activity
  - Continuing to perform the function of the original program but modifying the function to perform malicious activity (e.g., a Trojan horse version of a login program that collects passwords) or to disguise other malicious activity (e.g., a Trojan horse version of a process listing program that does not display certain processes that are malicious)
  - Performing a malicious function that completely replaces the function of the original program
- May be part of a Scam, like the Tech Support scams →

Apple Platform Security

** ACCESS TO THIS PC HAS BEEN BLOCKED FOR SECURITY REASONS **

Your computer has alerted us that it has been infected with a Trojan Spyware. The following data has been compromised.

> Email Credentials
> Banking Passwords
> Facebook Login

Call Apple Support: +1-(888)-598-1424 (Toll Free)

macOS Security

Trojan Spyware Alert - Error Code: #0x898778
Access to this PC has been blocked for security reasons.
Contact Mac Support: +1-(888)-598-1424 (Toll Free)

Threat Detected - Trojan Spyware
App: Ads.financetrack(1).exe

macOS Support
+1-(888)-598-1424 (Toll Free)

CalPolyPomona | 7 Dr. Valerio Formicola

Trojan Horses

A Trojan horse is a useful, or apparently useful, program or utility containing hidden code that, when invoked, performs some unwanted or harmful function.

Trojan horse programs can be used to accomplish functions indirectly that the attacker could not accomplish directly. For example, to gain access to sensitive, personal information stored in the files of a user, an attacker could create a Trojan horse program that, when executed, scans the user's files for the desired sensitive information and sends a copy of it to the attacker via a Web form or e-mail or text message. The author could then entice users to run the program by incorporating it into a game or useful utility program, and making it available via a known software distribution site or app store. This approach has been used recently with utilities that "claim" to be the latest anti-virus scanner, or security update, for systems, but which are actually malicious Trojans, often carrying payloads such as spyware that searches for banking credentials. Hence, users need to take precautions to validate the source of any software they install.

Trojan horses fit into one of three models:

• Continuing to perform the function of the original program and additionally performing a separate malicious activity

• Continuing to perform the function of the original program but modifying the function to perform malicious activity (e.g., a Trojan horse version of a login program that collects passwords) or to disguise other malicious activity (e.g., a Trojan horse version of a process listing program that does not display certain processes that are malicious)

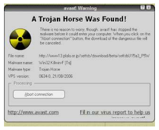
• Performing a malicious function that completely replaces the function of the original program

Some Trojans avoid the requirement for user assistance by exploiting some software vulnerability to enable their automatic installation and execution. In this they share some features of a worm, but unlike it, they do not replicate. A prominent example of such an attack was the Hydraq Trojan used in Operation Aurora in 2009 and early 2010. This exploited a vulnerability in Internet Explorer to install itself, and targeted several high-profile companies. It was typically distributed using either spam e-mail or via a compromised website using a “watering-hole” attack

Digital Technique: Trojan Horses Types (2/3)

BlackBerry.
Intelligent Security. Everywhere.
Decade of the
RATs
Cross-Platform APT Espionage Attacks
Targeting Linux, Windows and Android

- **Remote Access Trojans (RATs):**
  - Remote Access Trojans are today better known as Remote Administration Tool. They provide full access over victim's system to attackers and enable him/her to remotely access files, private conversations, transactional data etc.
- **Data Sending Trojans:**
  - These Trojans are used for stealing information like passwords, credit card numbers, companies private and confidential data etc. They do this by installing keystroke loggers in system and send record to attacker via ftp or emails.
- **Destructive Trojans:**
  - As name suggests these are written solely for destructive purposes and can destroy OS by deleting core files of system.
- **Denial Of Service DoS Attack Trojans:**
  - They enable an attacker to launch a Distributed Denial Of Service(DDoS) attack against another victim.
- **Proxy Trojans:**
  - These Trojans turn victim's PC into a proxy server for attacker, enabling him/her to do any malicious activity online with full anonymity.
- **FTP Trojans:**
  - These allow attacker to connect victim as a FTP server due to which he can download all files in victim PC using port 21.
- **Security Disablers:**
  - These are a special kind of Trojans specially used to attack security measures in victim PC.


avast! Warning

A Trojan Horse Was Found!

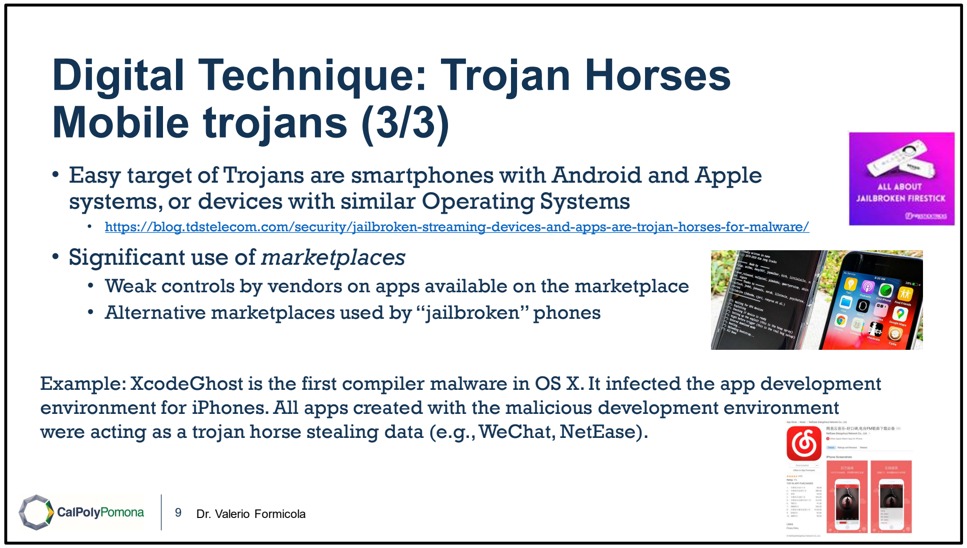
There is no reason to worry, though. avast! has stopped the malware before it could enter your computer. When you click on the "Abort connection" button, the download of the dangerous file will be canceled.

File name: http://www13.plala.or.jp/settsb/download/beta/settsbU15a3_PSW/

Malware name: Win32:Killwin-F [Trj]

Malware type: Trojan Horse

VPS version: 0634-0, 21/08/2006



Digital Technique: Trojan Horses Mobile trojans (3/3)

- Easy target of Trojans are smartphones with Android and Apple systems, or devices with similar Operating Systems
  - https://blog.tdstelecom.com/security/jailbroken-streaming-devices-and-apps-are-trojan-horses-for-malware/
- Significant use of *marketplaces*
  - Weak controls by vendors on apps available on the marketplace
  - Alternative marketplaces used by "jailbroken" phones

Example: XcodeGhost is the first compiler malware in OS X. It infected the app development environment for iPhones. All apps created with the malicious development environment were acting as a trojan horse stealing data (e.g., WeChat, NetEase).

CalPolyPomona | 9 | Dr. Valerio Formicola

Mobile phone Trojans also first appeared in 2004 with the discovery of Skuller. As with mobile worms, the target is the smartphone, and the early mobile Trojans targeted Symbian phones. More recently, a significant number of Trojans have been detected that target Android phones and Apple iPhones. These Trojans are usually distributed via one or more of the app marketplaces for the target phone O/S.

The rapid growth in smartphone sales and use, which increasingly contain valuable personal information, make them an attractive target for criminals and other attackers. Given five in six new phones run Android, they are a key target [SYMA16]. The number of vulnerabilities discovered in, and malware families targeting these phones, have both increased steadily in recent years. Recent examples include a phishing Trojan that tricks the user into entering their banking details, and ransomware that mimics Google's design style to appear more legitimate and intimidating.

The tighter controls that Apple impose on their app store, mean that many iPhone Trojans target "jail-broken" phones, and are distributed via unofficial sites. However a number of versions of the iPhone O/S contained some form of graphic or PDF vulnerability. Indeed these vulnerabilities were the main means used to “jailbreak” the phones. But they also provided a path that malware could use to target the phones. While Apple has fixed a number of these vulnerabilities, new variants continued to be discovered. This is yet another illustration of just how difficult it is, for even well- resourced organizations, to write secure software within a complex system, such as an operating system. We will return to this topic in Chapters 10 and 11. More recently in 2015, XcodeGhost malware was discovered in a number of legitimate Apple Store apps. The apps were not intentionally designed to be malicious, but their developers used a compromised Xcode development system that covertly installed the malware as the apps were created [SYMA16]. This is one of several examples of attackers exploiting the development or enterprise provisioning infrastructure to assist malware distribution.

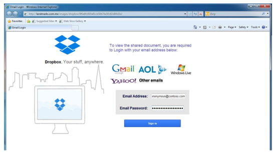
https://www.lookout.com/threat-intelligence/article/xcodeghost-apps

Definition:

To jailbreak a phone is to modify it so that you can enjoy unrestricted access to the entire file system. This access allows for changes that aren't supported by the phone in its default state. When the phone is free from certain bounds set by the manufacturer or wireless carrier, the device owner gains more control over the device, including how it performs. Devices that are commonly jailbroken are the iPhone, iPod touch, and iPad, but many people are now jailbreaking devices like the Roku stick, Fire TV, and Chromecast. Jailbreaking an Android device is normally called rooting.

https://blog.tdstelecom.com/security/jailbroken-streaming-devices-and-apps-are-trojan-horses-for-malware/

Digital Technique: Credential Harvesting

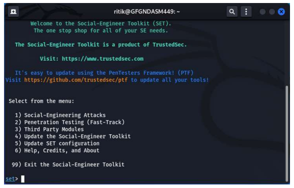

Email Login - Windows Internet Explorer
http://landmarks.com.mx/images/dropbox/9f6e6fc600e81cb58b74e50c62d84d3a/
Bing
Favorites
Suggested Sites
Web Slice Gallery
Email Login
Page
Safety
Tools
Dropbox. Your stuff, anywhere.
Gmail
AOL
Windows Live
YAHOO!
Other emails
Sign in

To view the shared document, you are required to Login with your email address below:

Email Address: inonymous@contoso.com

Email Password: ••••••••••••••••••

- *Credential harvesting* is the process of gathering credentials like logins, usernames and passwords.
  - Credential harvesters are often combined with another type of attack, like phishing or web attacks, during which credentials from a compromised site may be sent to a centralized location controlled by malicious actors.
  - A credential harvester attack is an attack that targets information stored on computers. When successful, this type of hack leads to the theft of a person's username and password. And although it doesn't lead to stealing any private data, it jeopardizes any kind of service that requires authentication, such as Facebook or email account.



```
      Welcome to the Social-Engineer Toolkit (SET).
       The one stop shop for all of your SE needs.

   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>
```

- User awareness and Multifactor authentication (MFA) are valid strategy of defense.

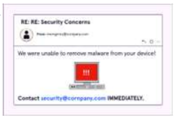
https://www.geeksforgeeks.org/what-is-credential-harvester-attack/

In-Person techniques of social engineering

- *Dumpster diving:* retrieving potentially sensitive information from a dumpster. Dumpster diving can provide treasure troves of information about an organization, including documentation and notes. Organizations that want to avoid this will secure their dumpsters, use secure disposal services for documents.
- *Shoulder surfing:* is the process of looking over a person's shoulder to capture information like passwords or other data. Although shoulder surfing typically implies actually looking over a person's shoulder, other similar attacks such as looking into a mirror behind a person entering their credentials would also be considered shoulder surfing. Preventing shoulder surfing requires awareness on the part of potential targets, although tools like polarized security lenses over mobile devices like laptops can help prevent shoulder surfing in public spaces.
- *Tailgating:* is a physical entry attack that requires simply following someone who has authorized access to an area so that as they open secured doors you can pass through as well. Much like shoulder surfing, tailgating is best prevented by individual awareness. If someone attempts to follow you through a secure door, you should make them present their own credentials instead of letting them in or report the intrusion immediately!

- *Eliciting information:* often called elicitation, is a technique used to gather information without targets realizing they are providing it. Techniques like flattery, false ignorance, or even acting as a counselor or sounding board are all common elements of an elicitation effort. Talking a target through things, making incorrect statements so that they correct the person eliciting details with the information they need, and other techniques are all part of the elicitation process.

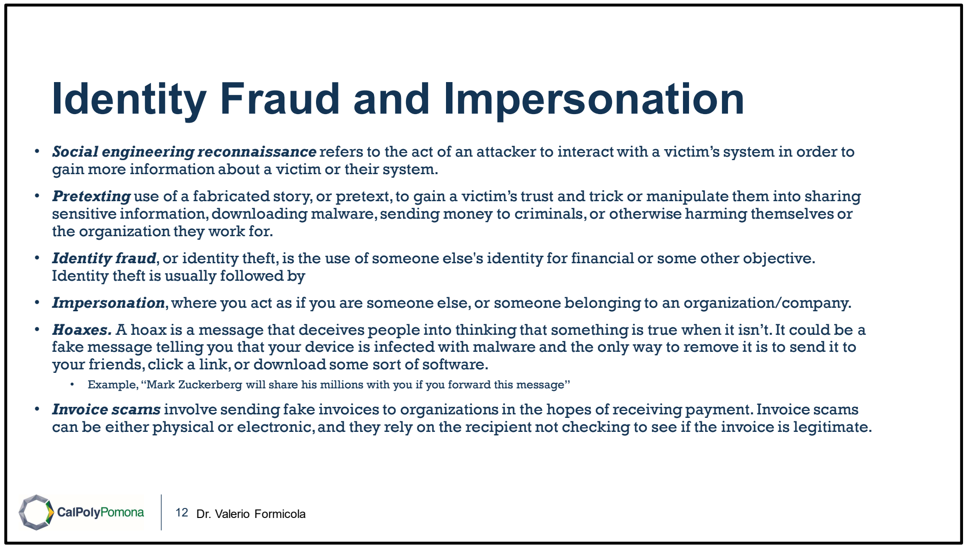
- *Prepending:* attacker prepends, or attaches, a trustworthy value like "RE:"
  or "MAILSAFE: PASSED" to a message in order to make the message appear more trustworthy.



RE: RE: Security Concerns

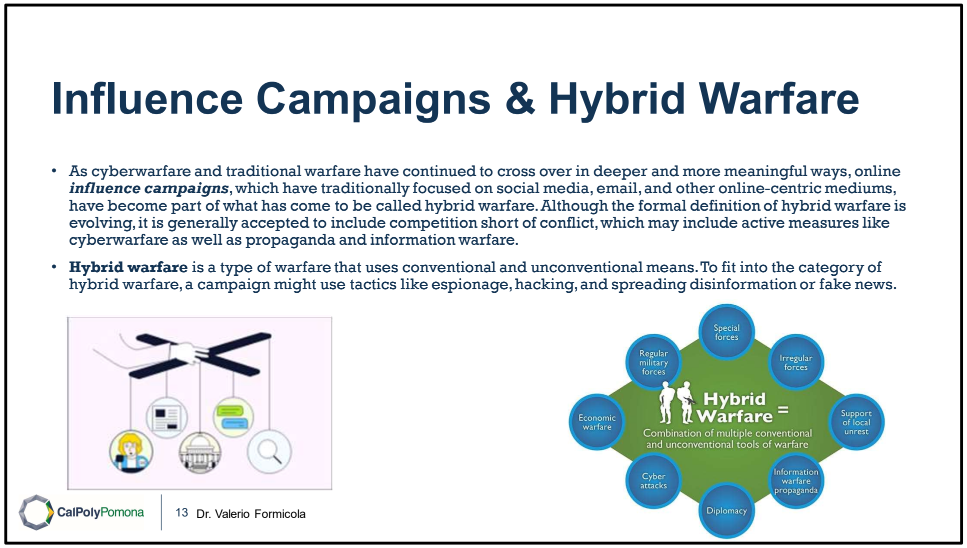
We were unable to remove malware from your device!

Contact security@company.com IMMEDIATELY.



Identity Fraud and Impersonation

- ***Social engineering reconnaissance*** refers to the act of an attacker to interact with a victim's system in order to gain more information about a victim or their system.
- ***Pretexting*** use of a fabricated story, or pretext, to gain a victim's trust and trick or manipulate them into sharing sensitive information, downloading malware, sending money to criminals, or otherwise harming themselves or the organization they work for.
- ***Identity fraud***, or identity theft, is the use of someone else's identity for financial or some other objective. Identity theft is usually followed by
- ***Impersonation***, where you act as if you are someone else, or someone belonging to an organization/company.
- ***Hoaxes.*** A hoax is a message that deceives people into thinking that something is true when it isn't. It could be a fake message telling you that your device is infected with malware and the only way to remove it is to send it to your friends, click a link, or download some sort of software.
  - Example, "Mark Zuckerberg will share his millions with you if you forward this message"
- ***Invoice scams*** involve sending fake invoices to organizations in the hopes of receiving payment. Invoice scams can be either physical or electronic, and they rely on the recipient not checking to see if the invoice is legitimate.



Influence Campaigns & Hybrid Warfare

- As cyberwarfare and traditional warfare have continued to cross over in deeper and more meaningful ways, online ***influence campaigns***, which have traditionally focused on social media, email, and other online-centric mediums, have become part of what has come to be called hybrid warfare. Although the formal definition of hybrid warfare is evolving, it is generally accepted to include competition short of conflict, which may include active measures like cyberwarfare as well as propaganda and information warfare.
- **Hybrid warfare** is a type of warfare that uses conventional and unconventional means. To fit into the category of hybrid warfare, a campaign might use tactics like espionage, hacking, and spreading disinformation or fake news.

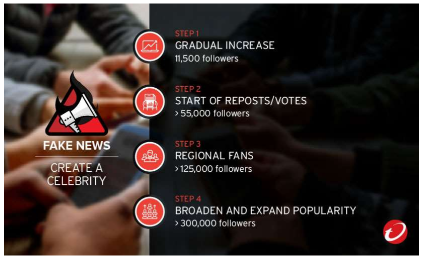
CalPolyPomona 13 Dr. Valerio Formicola

Cyberwarfare is the use of cyber attacks against an enemy state. The objective is usually to cause harm as a component of, prelude to, or proxy for actual warfare.[1] Some intended outcomes could be espionage, sabotage, propaganda, manipulation or economic warfare.

Influence campaigns themselves are not the exclusive domain of cyberwarfare, however. Individuals and organizations conduct influence campaigns to turn public opinion in directions of their choosing. Even advertising campaigns can be considered a form of influence campaign, but in general, most influence campaigns are associated with disinformation campaigns.

Fake news and influential campaigns

false stories that appear to be news, spread on the internet or using other media, usually created to influence political views or as a joke



FAKE NEWS

CREATE A CELEBRITY

STEP 1
GRADUAL INCREASE
11,500 followers

STEP 2
START OF REPOSTS/VOTES
› 55,000 followers

STEP 3
REGIONAL FANS
› 125,000 followers

STEP 4
BROADEN AND EXPAND POPULARITY
› 300,000 followers

The Hacker News

Your Retirement Road Map - Learn 4 Critical Milestones

Someone Hijacked MEGA Chrome Extension to Steal Users' Passwords

Malicious MEGA Chrome Extension Steals Passwords

Popular News

Build modern conversational

Fake news

Deep fake