CYBER SECURITY

The First Line of Defense in this New Age of Security Risks

Vito Rocco, Senior Information Security Analyst
University of Nevada, Las Vegas

UNLV | Office of INFORMATION TECHNOLOGY

About the Speaker

- Over 20 years in the InfoSec field
- 15 years military / DoD Red Team member and manager
- Security Consultant / Penetration Tester
- Digital Forensic Expert Witness
- CISSP, CCFP, GCFE, GPEN, CEH, EnCE, Sec+
- With UNLV since 2013

Standard Disclaimer

All views presented are my own and do not necessarily represent the views of The University of Nevada, Las Vegas or the Nevada System of Higher Education.

OVERVIEW

I. Importance of Information Security

I. Threats to security
   A. Types of threats
   B. How to recognize them

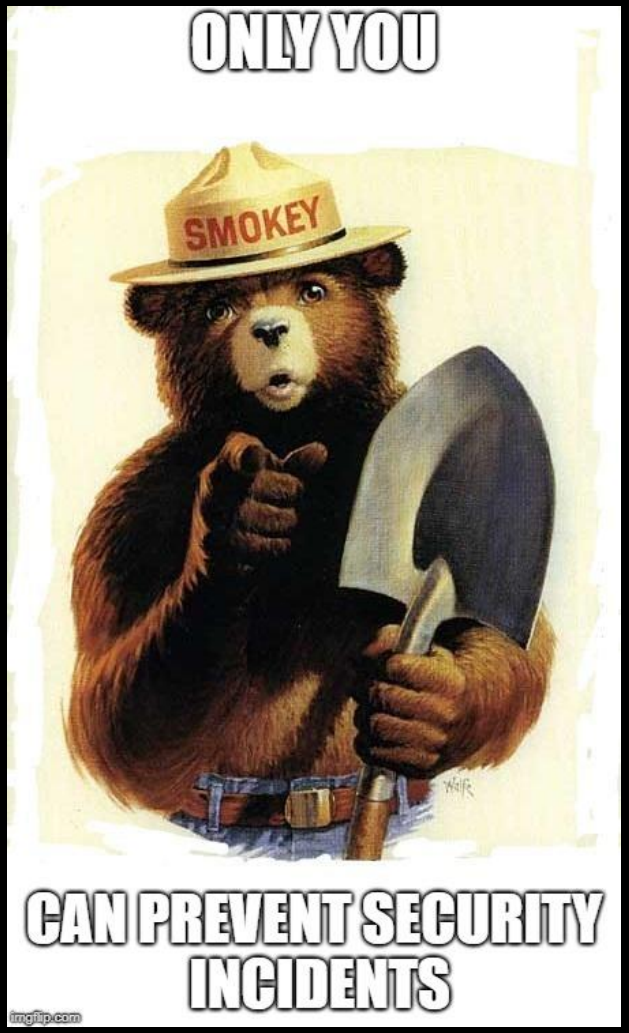
I. Best practices for Information Security

I. Q&A

IMPORTANCE OF SECURITY

- The internet allows an attacker to attack from anywhere on the planet.
- Risks caused by poor security knowledge and practice:
  - Identity Theft
  - Monetary Theft
  - Legal Ramifications (for yourself and/or your employer)
  - Possible termination if company policies are not followed
- Cyber Criminals have taken to targeting users rather than software or hardware as a means of gaining access to organizations.

SECURITY IS EVERYONE'S RESPONSIBILITY



LEADING THREATS

- Malware
- Ransomware
- Crypto-Mining
- Malicious Websites
- Drive-by Downloads
- Social Engineering / Phishing

UNLV | Office of INFORMATION TECHNOLOGY

MALWARE

- Broad category that includes, viruses, worms, trojans, rootkits, logic bombs, ransomware, crypto-miners, etc.
- Combination of “MAL” (bad) and “software”
- Can be installed in a number of ways and subvert the computer in several ways

RANSOMWARE

UNLV | Office of INFORMATION TECHNOLOGY

CRYPTO-MINING

- This type of malware uses your computer's processing power to mine crypto-currency (e.g. Bitcoin, Litecoin, Monero)
- These malware programs have become more prevalent as the prices of crypto currency have increased.
- Often more profitable for attackers than Ransomware because the income is guaranteed.
- They have the potential to slow down your computer, network, or applications and possibly even leak sensitive information from your system.

MALICIOUS WEBSITES

- Attempts to install malware onto your device.
- Usually requires some action on your part, however, in the case of a drive-by download, the website will attempt to install software on your computer without asking for permission first.
- Often look like legitimate websites.
- Might ask for permission to install one program, but install a completely different one -- one that you definitely do not want on your computer.

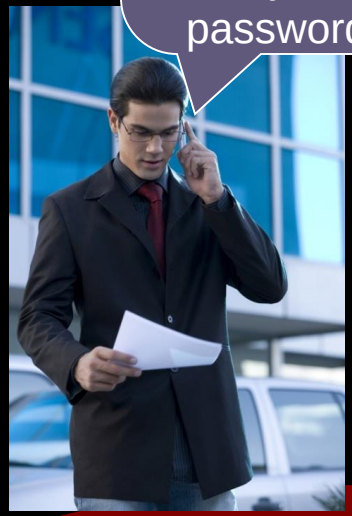
DRIVE-BY DOWNLOADS

- Can be installed on your computer simply by looking at an email, browsing a website or clicking on a pop-up window with text designed to mislead you, such as a false error message.
- Anti-virus software might be incapable of detecting it, because hackers deliberately make it difficult for anti-virus software to detect.
- Often doesn't require your consent, or tricks you into giving it.
- Might even be a website you've visited hundreds of times and trust, but somehow was compromised.

SOCIAL ENGINEERING

- Social engineering manipulates people into performing actions or divulging confidential information. Similar to a confidence trick or simple fraud, the term applies to the use of deception to gain information, commit fraud, or access computer systems.

Phone Call: This is John, the System Admin. What is your password?



In Person: What ethnicity are you? Your mother's maiden name?

Email: ABC Bank has noticed a problem with your account…

I have come to repair your machine…

and have some software patches

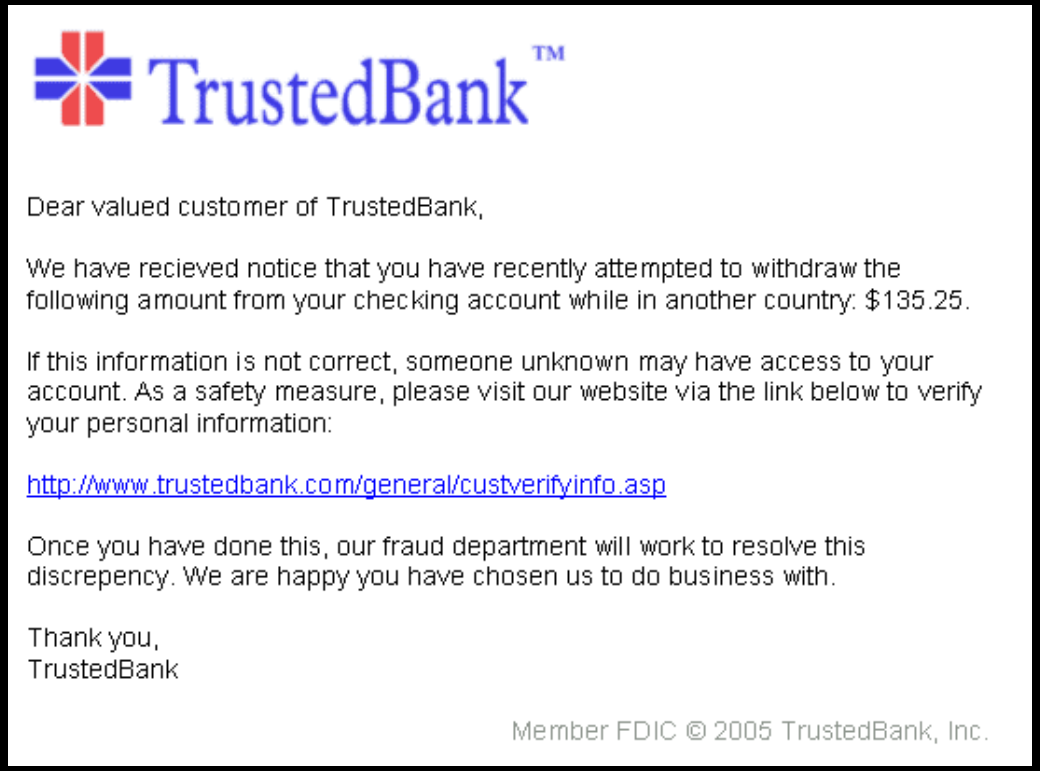
SOCIAL ENGINEERING

PHISHING = FAKE EMAIL

- **Phishing**: a 'trustworthy entity' asks via e-mail for sensitive information such as SSN, credit card numbers, login IDs or passwords.

UNLV | Office of INFORMATION TECHNOLOGY

PHARMING = FAKE WEB PAGES



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.

The link provided in the e-mail leads to a fake website, which often looks exactly like the real site, which collects important information and submits it to the attacker.

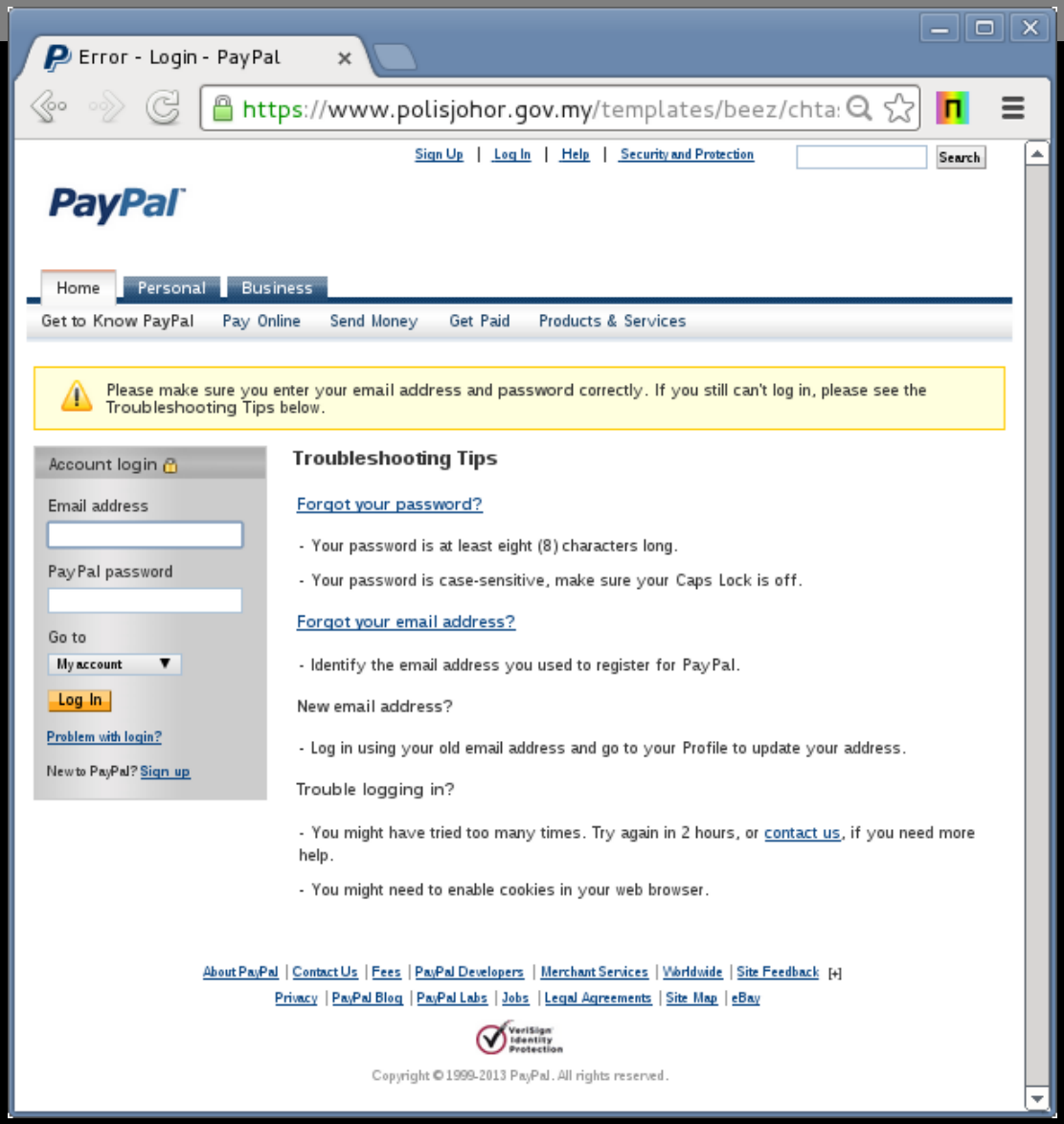
RECOGNIZING MALWARE/COMPROMISE

- Symptoms:
  - Antivirus software detects a problem
  - Pop-ups suddenly appear
  - Disk space disappears
  - Bad/slow system performance
  - Change to your browser homepage/start page
  - Files appear that should not be there
  - Unusual messages, sounds, or displays on your monitor
  - Your mouse moves by itself
  - Your computer shuts down and powers off by itself
  - Lots of network or disk activity while not particularly active

RECOGNIZING MALICIOUS WEBSITES

- Biggest clue will be the URL for the site
  - URLs follow the format https://domain.tld
  - chase.credit.com is not the same as credit.chase.com

- Look for the lock icon in the address bar or at the bottom of the page showing the site has a valid SSL certificate
  - Make sure the certificate matches the site you think you are visiting
  - Criminals use SSL certificates too!



UNLV | Office of INFORMATION TECHNOLOGY

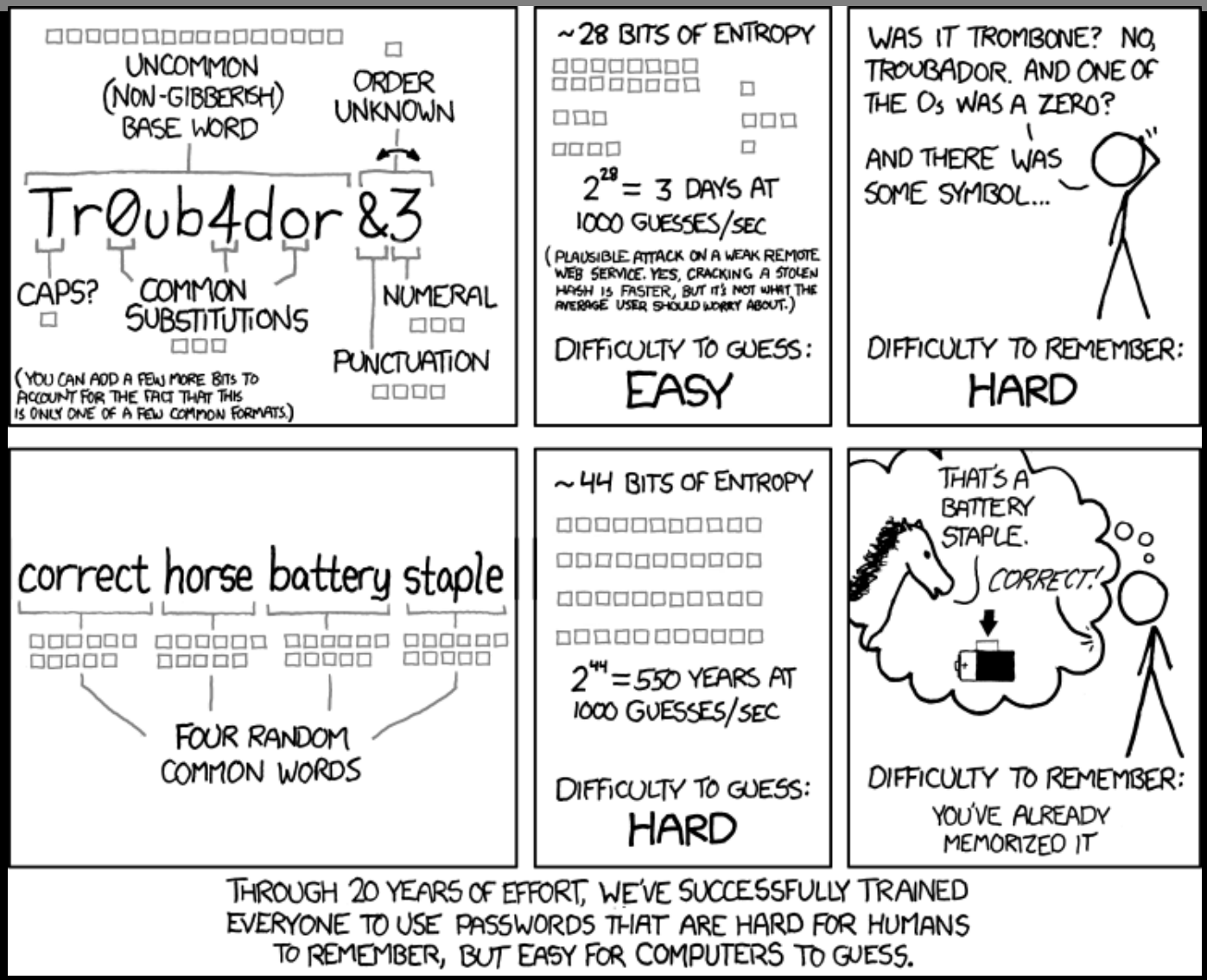
AVOID SOCIAL ENGINEERING & MALICIOUS SOFTWARE/WEBSITES

- Do not open email attachments unless you are expecting the email with the attachment and you trust the sender.
- Do not click on links in emails unless you are absolutely sure of their validity.
- Only visit and/or download software from websites you know and trust.
- Be skeptical of things that are “too good to be true.”

PASSWORD RECOMMENDATIONS

- A good password is:
  - **private**: it is used and known by one person only
  - **secret**: it does not appear in clear text in any file or program or on a piece of paper pinned to the terminal
  - **easily remembered**: so there is no need to write it down***
  - **not guessable**: by any program in a reasonable time
  - **changed regularly**: a good change policy is every 3 months
  - **unique**: don't reuse passwords on multiple sites
  - **long and complex**: at least 10 characters and a mixture of at least 3 of the following: upper case letters, lower case letters, digits and punctuation

***Use a password manager



*source: xkcd.com

BACK-UP IMPORTANT INFORMATION

- No security measure is 100%
- What information is important to you?
- Is your back-up:
  - Recent?
  - Off-site & Secure?
  - Tested?
  - Encrypted?

QUESTIONS?

Vito Rocco - vito.rocco@unlv.edu