Certified Ethical Hacker, Social Engineering and Phishing

CS4HS Cybersecurity Virtual Workshop

About Me

BSE in Social Studies Secondary Education.

BA in Computer Information Systems

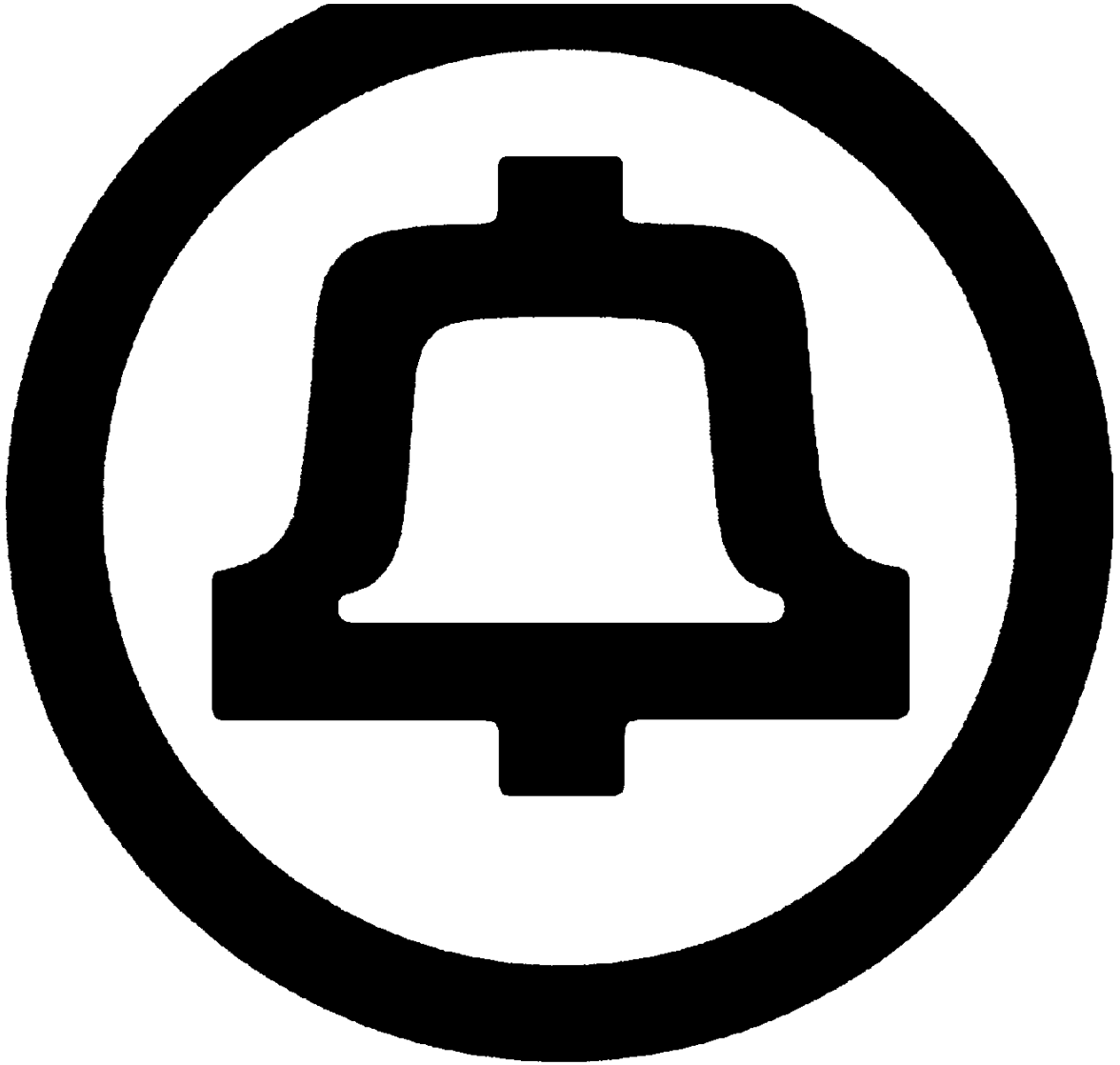
MS in Data Science

I am programmer/analyst and MS SQL Server Database Administrator and Oracle Database SQL Developer.

Adjunct professor at Buffalo State College teaching C++, Android Java and database programming.

WHY

Why study ethical hacking, social engineering and phishing?



The Bell Telephone Company

Hackers

The phone company had “hackers” working for them, appropriating computer languages and mainframe computers to create new technology.

The phone company also had “hackers” outside the company that were using technology such ”tone generators” to make free phone calls, and were intent on learning how the phone system worked.

UNIX and the B Programming Language

- In 1969 the first version of the operating system **UNIX** is released. UNIX is a multi-tasking, multi-user operating system developed by Ken Thompson, Dennis Ritchie, Brian Kernighan, Douglas McIlroy, Michael Lesk and Joe Ossanna, while they were working for AT&T laboratories. Ken Thompson created a programming language called “B” named after Bell laboratories or his wife Bonnie. The B language was based on an even earlier language called BCPL (**B**asic **C**ombined **P**rogramming **L**anguage).

“Don’t Reinvent the Wheel”

- Also in the late 1960s Dennis Ritchie and Brian Kernighan developed the C programming language while working for Bell/AT&T laboratories. The C programming language was developed to write full scale applications on operating systems. The C programming language along with the UNIX operating system quickly became popular on academic campuses such as Berkley, Dartmouth, MIT, Harvard, etc.

Phone Phreaks and Hackers

- Outside of the Bell phone company existed a group of technology enthusiasts that would come to be known as “Phone Phreaks” or “Hackers.” John Draper known as “Captain Crunch” was the most famous Phone Phreaker.
- The original meaning of the word “hacker” was someone who liked to take things apart, find out how they worked, improve them or modify them to their own needs.
- People began exploring the Bell telephone network because it was the most complex system in existence at the time.

Hacking

- Phone phreaking would also attract the attention of Steve Jobs and Steve Wozniak who would later go on to form Apple computer.

Certified Ethical Hacker

- Certified ethical hackers look for weaknesses and vulnerabilities in computer systems.

- They used to be called “white hat” hackers, a nod to old Western movies where the good guy would wear a white hat and the villain would wear a black hat.

Hackers

Prior to the rise of certified ethical hacking as a career, hackers would often get hired as consultants working for the companies that they had exploited.

The most famous example of a hacker is Kevin Mitnick, who hacked into phone companies and computer software firms in the 1980s and 1990s. He would spend many years in jail or on the run for his hacking.

CEH Certification

- Fee: $1,199
- 4-hour exam
- $80 annual renewal fee.
- Good for three years

What does a Certified Ethical Hacker do?

Vulnerability Assessment and “pen” or Penetration Testing:

Log reviews

Test or “synthetic” transactions to the the system, especially security.

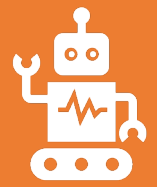
Software vulnerability assessment – code review

Misuse case testing

Certified Ethical Hacker

- Test case assessment
- Risk, Threat and Vulnerability Assessment

Vulnerability Scanning



Automated, passive testing of security controls.

Identify vulnerabilities, lapses in security controls and identify system misconfigurations.

Certified Ethical Hacker

- NVD – National Vulnerability Database. Security measurement and compliance.

- CVE – Common Vulnerabilities and Exposure database.

Cyber Attack Types

- Physical impersonation – dressing up like a security guard, janitor or other employee to gain entry to a site.
- Zero Day attacks – exploiting a vulnerability in computer code before it becomes known to the general IT community.

Cyber Attack types

SPIM – SPAM messages targeting Instant Message (IM) users.

Pharming – redirecting a web site’s traffic to another website.

Phishing – asking for user credentials.

Cyber Attack Types

- MITM – Man in the Middle Attacks. Here a hacker gets in the ”middle” of computer communication between two users directs or alters the exchange without the knowledge of the two parties.

Social Engineering

- **Social engineering** is the deceptive methods that malicious individuals use to compromise computer systems using the inherent weaknesses of the system's operators.

Why use Social Engineering?

- Cheaper
- Less Complicated
- Readily available
- Safer

The Spanish Prisoner

The “Spanish Prisoner” letter was a scam in the 1500’s where the author claimed to be in prison, and if they obtained money, they would pay it back several times over.

Willingness to help

Greed

Cyber Attack Types

Shoulder surfing – looking over someone's shoulder to get a password or pin.

Dumpster diving – looking through someone's trash for information.

Tailgating – gaining physical entry to a site by following an employee through a gate or a door.

Pretexting

A malicious attacker will pretend o be someone else to gain access to sensitive data.

A person will pretend to be from the Help Desk or someone in a position of higher authority using the phone, text, or email.

Email Spoofing – email appears to be from a legitimate source.

Pretexting takes advantage of deal to carry out job duties, willingness to help and gullibility.

Pretexting

- Employees may be hesitant to challenge an individual out of fear of offending that person or being disrespectful.
- Tailgating or “piggybacking” can be mitigated using identity badges, access cards and biometrics.
-

Shoulder Surfing

A malicious person acquires sensitive data using a surveillance method.

Surveillance can range from peering over a person's shoulder, using hidden cameras, keystroke loggers or ATM skimmers.

The objective is to steal login credentials or credit/debit card details.

Shoulder surfing takes advantage of a sense of security and inattentiveness.

Dumpster Diving

A Malicious person looking through disposed items (like garbage) to find sensitive data that was not disposed of properly.

- ❑ Documents that were not properly shredded.
- ❑ Hardware devices that were not overwritten or “blanked out.”

Dumpster Diving

DUMPSTER DIVING TAKES ADVANTAGE OF A FALSE SENSE OF SECURITY AND NEGLIGENCE.

PEOPLE FIGURE NO ONE WILL TAKE THE TIME AND EFFORT TO GO THROUGH THE GARBAGE.

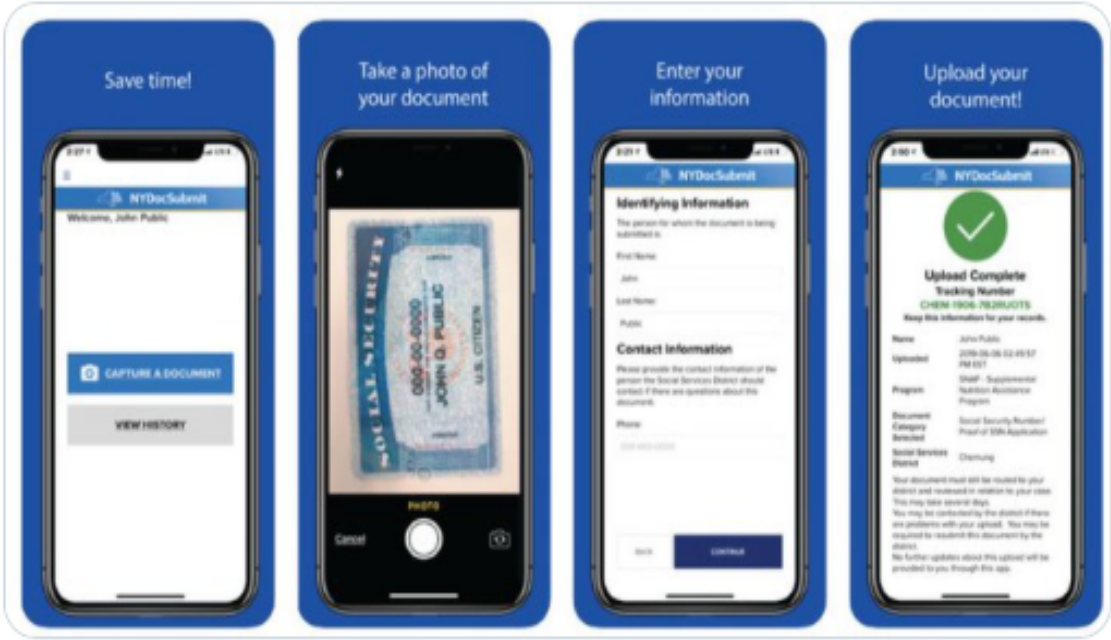
Dumpster Diving

- Paper documents can be properly disposed of using horizontal and vertical shredding and possibly burning.

Dumpster Diving

There is new threat of “virtual” dumpster diving as government and businesses increasingly use e-forms to take the place of paper forms and manual submissions.

The @ECSocServices is pleased to announce the launch of Mobile Document Upload for Temporary Assistance, SNAP (food stamps), Medicaid, and HEAP clients. Clients can now photograph documents and submit them to ECDSS from their Apple or Android device. More: www2.erie.gov/socialservices...



Rogue Access Points

Access points are wireless connections to computer networks.

If a user sees a network such as “TellMyWiFiLoverHer” without the lock symbol signifying WEP, WPA, WPA2 wireless protocols, it may be a “rogue access point.”

Browsing history, user details and sensitive information can be intercepted using these bogus access points.

Phishing

Part of the Online Data Security AP CSP principles.

PII - Personally Identifiable Information. Data such as names and addresses stored on computers and flowing through the internet that can identify you.

Phishing

“Hackers commonly replace the letter *f* with *ph*, a nod to the original form of hacking known as phone phreaking. Phreaking was coined by John Draper, aka Captain Crunch, who created the infamous Blue Box that emitted audible tones for hacking telephone systems in the early 1970s.”

Phishing

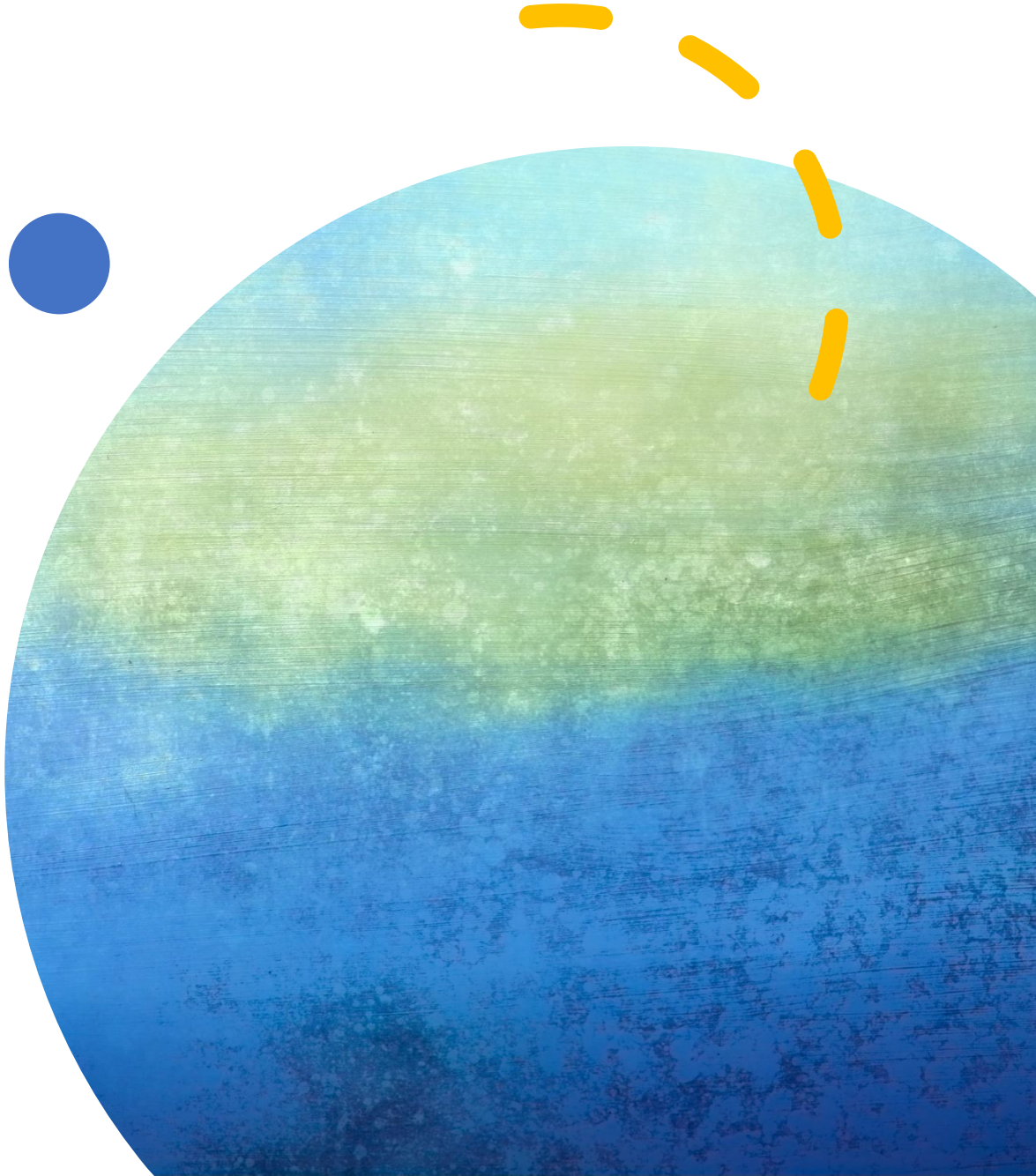
Older users will often say “How can they know all of this information?”

While younger users will just assume that they don’t in fact have any privacy in this digital age where there is so much information online.

Geolocation

Geolocation is the position of the user’s desktop computer, laptop, phone or fitness tracking devices.

Geolocation can be determined using very precise GPS and the less precise IP-based geolocation.



Geolocation

- Geolocation information is very useful in getting directions and tracking fitness activities but can be used to harass and stalk individuals.

Wi-Fi Positioning System

A device with a Wi-Fi antenna scans for Wi-Fi access points and measures the strength of the signal.

The device then uses a database of access point locations to determine its location based on the Wi-Fi access points and signal strength.

IP-based geolocation

- Every time a device such as a computer or smartphone sends information over the internet it also sends the IP address of that device.

Cell Tower Trilateration

- A cell tower can estimate the distance between the cell tower and the smartphone by measuring the round-trip delivery time of the signal and the strength of the phone signal.

Cookies

- Websites often use *cookies* – small text files stored on a computer that helps a website track a user across multiple web pages and offer personalized content on that web site.

- When accessing a web site a browser will send an HTTP request to the server hosting the web site.
- The server will then create a cookie in the local computer drive with the cookie session ID and a cookie expiration date – when the cookie will be removed by the browser from the computer.

Cookies

- Cookies can be ***session cookies*** – small text files that are deleted when the user ends the browser session, or ***persistent cookies*** that remain on the computer even if the computer is turned off.

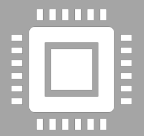
- Cookies can be used to track a user's web browsing and may hold user information such as a user ID if logged on to a search site such as Google or Yahoo.

Cookies

Many websites warn users that they use cookies and have a cookie policy that can be reviewed.

Browsing History

Browsers store information about searches users make every day.



Such information such as the search query, date, time, IP address and user agent are collected.

Other details such as user IDs and cookies might also be collected if a user is logged on to the search engine website.

Browsers

- Browsers such as DuckDuckGo do not store IP addresses, cookies or user agents.

Explicit Emails

Explicit email use information bought cheaply on the dark web to send out emails with explicit user details, such as old passwords.

This really gets the attention of the person received the email since passwords are often re-used on different sites or changed only slightly.

Phishing

Phishing – the act of acquiring sensitive data through electronic communications by pretending to be a credible source

Phishing

MOST PHISHING IS DONE USING EMAILS. IT IS RELATIVELY SIMPLE TO SPOOF A LEGITIMATE ORGANIZATION'S LOGO AND CREATE AN EMAIL ADDRESS THAT LOOKS CONVINCING.

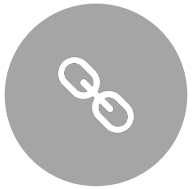
GENERIC OR MISSING GREETING.

DECEPTIVE EMAIL ADDRESS.

REQUEST TO VERIFY ACCOUNT

SENSE OF URGENCY

ATTACHMENTS



STRANGE LOOKING LINKS

Phishing

PRIZE OR AWARD NOTIFICATION

MISSPELLINGS, GRAMMAR MISTAKES OR ODD WORDING.

Twitter

Phishing attempts often ask for payment in Bitcoin or other cryptocurrencies to avoid being tracked.

Spear Phishing

- Sending targeted emails to recipients pretending to be a trusted source. These phishing attempts are more researched and may contain credible information that makes them seem more legitimate.

Recent Phishing Trends

- More personalization. Personal and company details are including in the subject and text of the emails.
- Multi-platform – phishing attacks are showing up in texts.
- HTTPS usage. Many malicious links are never using secure server URLs.
- BEC Business Email Campaigns.

Phishing – more complicated examples

Redirection using Local Host

Local Host – the default name of the computer. IP address 127.0.0.1

Using web server software and a fake web page along with a bit of PHP code, a user can be “redirected” to what appears to be a legitimate web site. The user is then prompted to enter their credentials which are sent to a text file.

Phishing using server redirection

Resources

- Hacking and Phone Phreaking
- http://www.youtube.com/watch?v=jnI0ndIF6BI

- Origin of Phishing word
- https://www.computerworld.com/article/2575094/sidebar--the-origins-of-phishing.html