Email and Hacking

- Email is a large attack vector.
- It is one of the oldest ways to infitrate system. Many attackers will harvest emails in order to send specially crafted emails to individuals they want to hack.
- Email protocols usually runs on port 25 or 587 and use SMTP (Simple Mail Transfer Protocol) to send and receive emails.

Types of Email Hacking

- Phishing - Sending an enticing fake email to convince a victim to click or download. Usually either to spot.
- Spear Phishing - targeted Phishing on an organization or individual. Much more specific to the organization or individual. Has a high success rate.
- Whaling - phishing email that targets high level employees and is much more specific to that individual. This has a very high success rate.
- Pharming - Two part hacking. An email click to entice (or frequently visited site) will rediret your website traffic to bogus website by changing DNS cache or host files.
- Cookie Theft - Email cna be used to convince a target to click a link that will steal the unencrypted stored cookie sessions, allowing the attacker access to any sites that are logged into.

Using email to hack a system falls into the social engineering category. Specially crafted emails can fool anyone. Keep in mind this does not make anyone who falls for such an attack "stupid". When fooling a customer this way they can become angry. Remember to *"educate and assist, not humiliate and win"*. - Chris Hadnagy

Federal Trade Commision Advice

Here's a video for advice on how to resolve email hacks. This video is foxused on "home" users. if a business or organization is hacked this way, there are other steps to recover and mitigrate.

[link here]

Email Header Analysis

There are many tools to analyze an email header. A quick Google search will return plenty. It is a good practice to check out the header to an email that you are unsure of.

For example, you are looking for a new pure bread Maltese pup, so you check out google Craigslist. You come across a great deal and email the individual. They respond with the emaik on the next slide.

- Email consists of several parts:

- Envelope - Has its own address information. Much like snail mail
- Body - consists of the message
- Header - contains the date, who sent the message, who received the message, user agents, IP Addresses, and the message ID.

The Email tracking service looks at email header information. When an email passes from server to server, the IP can be detected. Using this technuiqe, an attacker / pentester can determine the location of an individual when they sent an email.

This is not fool proof. - Many attackers can spoof (fake) an email location by modifying the header or using proxies.

Online web services will list the original Ip address„ the city the mail originated from, and the country of origin. The header will also provide the latitude and longitude for the originating server.