Internet Security Training

Prepared by
Sgt. Gibbs, Thomas B. 82-11

Community Partnerships

- Collaborative partnerships between the law enforcement agency and the individuals and organizations they serve to develop solutions to problems and increase trust in police.

- In order for law enforcement agencies to be effective they have to work hand in hand with the communities they serve.

Internet Security

Social Engineering

- Refers to psychological manipulation of people into performing actions or divulging information
- Examples can be seen on TV show Burn Notice
- Many different types of social engineering

Pretexting

- The act of creating and using an invented scenario (the pretext) to engage a victim in a manner which increases the chances the victim will divulge information or to perform actions that would not normally be performed

- Can be used to impersonate co-workers, supervisors, police, bank, or any position of authority perceived by the victim

Phishing

- Phishing is a technique used to obtain private information.
- Usually done by phone or e-mail
- E-mails may appear to be from a legitimate business and request verification of information. E-mail usually contain a link to a fraudulent web page which may seem legitimate containing company logos
- May also be done over the phone, usually phisher warns victim of dire consequence and asks for personal information for verification

Tailgating

- Involves an area secured by unattended access points into a restricted area
- Suspect looks official and simply walks in behind someone who has legitimate access
- The suspect may also fake the action of presenting credentials

Baiting

- Baiting is essentially a modern day Trojan Horse

- Suspect leaves media (USB, CD) infected with a virus or malware in an area likely to be found and waits for an unsuspecting victim to use the device

Malware (Malicious Software)

- Malware includes computer viruses, ransomware, trojan horses, rootkits, keyloggers, spyware, and the list goes on

- Malware is primarily used to steal vital information of person, financial, or business nature

- Infected computers can be used to send spam e-mail, store child pornography, or engage in DDS (Distributed Denial of Service Attacks)

Precautions you can take

- √ Do not conduct personal business on public computers or networks
- √ Avoid business transactions over open networks unless a VPN is established (Virtual Private Network) which will encrypt data
- √ Use Anti-Virus & Anti-Malware Software and conduct regular scans
- √ Be wary of opening e-mail attachments from unknown sources (phishing)
- √ Be mindful of social engineering tactics

QUESTIONS