Cybersecurity

Phishing and Spam

CYBER.ORG

Phishing

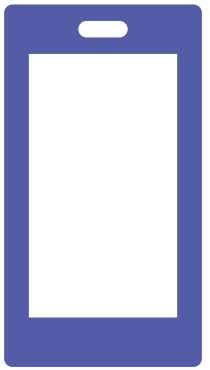
- Electronic social engineering
  - Often delivered by spam or via direct message
  - Can be convincing at times …or not
- Don’t be fooled
  - Check the URL
- Something is usually odd
  - Spelling, fonts, graphics, feeling

CYBER.ORG

Vishing

- Voice phishing
- Sometimes digital voice, sometimes real human
  - “Hello! You’ve won a free cruise!”
  - “This is the Federal Revenue Service calling. There is a fine against your name.”
  - “This is the police. You have a warrant for your arrest if you do not pay immediately.” “Yes, you can pay with Apple or Starbucks gift cards.”

Smishing



- SMS/Texting phishing
- Sent via a SMS text message
  - “Click here for $1000”
  - “Hey, you won the free jersey”
  - “You need to click here to pay your invoice”

CYBER.ORG

Spear Phishing

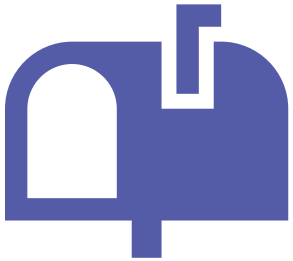
- Phishing a specific target directly
  - Focused attack versus wide “net”
- Uses inside information
  “Carlos in Accounting said…”
  “Janet in IT told me…”
- Directed attack is more believable
  - Spear phishing executives like CEO known as “whaling”
- Whaling - Directed towards high profile targets like CEO’s of companies

Pharming

- Does not require the user to click a link
- A malicious script hidden in a message
  - This link directs the user to a malicious website

- Pharming = A mix of Phishing and Farming

Spam



- Sending a message to thousands of people
- Large scale phishing attack
- SPIM - Spam over instant messenger
  - Sending spam via instant messenger app
    - i.e. Facebook messenger, Instagram DM, Discord, etc…
- Invoice Scam - Fake invoices sent as a phishing attack
  - You owe us $5,000 for late fees

CYBER.ORG

Famous Spear Phishing cases

- April 2011 – Epsilon
  - Less than 3,000 email addresses attacked
  - 100% of email operation staff
  - Downloaded anti-virus disabler, keylogger, and remote admin tool
- April 2011 – Oak Ridge National Laboratory
  - Email from the “Human Resources Department”
  - 530 employees targeted, 57 people clicked, 2 were infected
  - Data downloaded and servers infected with malware

The Big Phish

- March 19, 2016
- Target: John Podesta
  - Chief of Staff for Bill Clinton (‘98-’01)
  - Counselor to the President for Barak Obama (‘14-’15)
  - Chairman of Hillary Clinton’s 2016 campaign
- Personal Gmail account hacked
  - Messages from 2007 through 2016
- Gave over login information via link in following phishing email
  - What looks “off” about the email to you?

> Hi John
>
> Someone just used your password to try to sign in to your Google Account
> john.podesta@gmail.com.
>
> Details:
> Saturday, 19 March, 8:34:30 UTC
> IP Address: 134.249.139.239
> Location: Ukraine
>
> Google stopped this sign-in attempt. You should change your password
> immediately.
>
> CHANGE PASSWORD <https://bit.ly/1PibSU0>
>
> Best,
> The Gmail Team
> You received this mandatory email service announcement to update you about
> important changes to your Google product or account.

Filling the Net

- Podesta used the bit.ly link to “reset” his password
  - Shocker: *it wasn’t actually from Google*
- Ten years of personal emails were copied
- Email messages published on WikiLeaks
  - Exposed email exchanges caused huge uproar in 2016 presidential election cycle
- Culprits: Fancy Bear
  - Russian intelligence-backed hacker group [may be a silly name, they’re a serious group]
  - Also responsible for hacking DNC in 2016 presidential election