Recognizing Phishing Scams & Malware

Tobias Quosigk & Chris Gaddis
ITS Information Security Office
Cyber Security Awareness Day
Kennesaw State University
October 28, 2009

What is phishing?

- a scam by which an e-mail user is duped into revealing personal or confidential information which the scammer can use illicitly
  
  Source: Merriam-Webster’s dictionary

- has expanded to instant messaging, text messaging, social networking

- phishing via trojan malware programs on the rise
What is at risk?

- financial services accounts (banks, brokerages, credit cards, online payment services, ...)
- e-commerce accounts (online retailers, cell phone providers, ...)
- email accounts
- any data stored on your computer

Phishing in the News

- Google News
Who are the phishers?

- organized crime syndicates from around the globe
- smaller cartels
- individuals

SMS Phishing

- Text Messaging (SMS)

  - What are the red flags?
When in doubt...

- Do not reply to the text message, call the number referenced, or follow any links in the message.
- Call your bank at the number printed on your statement or the back of your credit/debit card to verify authenticity of the message.

Phishing Email

- From: account_verification_dept009@hotmail.com
- Subject: Hotmail Warning (Verify Your Hotmail Account now To Avoid It Closed)
- Date: Sun, 10 Aug 2008 19:28:54 +0000

Dear Account User

This Email is from Hotmail Customer Care and we are sending it to every Hotmail User Accounts Owner for safety. We are having congestions due to the anonymous registration of Hotmail accounts so we are shutting down some Hotmail accounts and your account was among those to be deleted. We are sending you this email to so that you can verify and let us know if you still want to use this account. If you are still interested please confirm your account by filling the space below. Your User name, password, date of birth and your country information would be needed to verify your account. Due to the congestion in all Hotmail users and removal of all unused Hotmail Accounts,Hotmail would be shutting down all unused Accounts. You will have to confirm your E-mail by filling out your Login Information below after clicking the reply button, or your account will be suspended within 24 hours for security reasons.

* Username: ..............................
* Password: ..............................
* Date of Birth: ..............................
* Country Or Territory: ...............  

After following the instructions in the sheet, your account will not be interrupted and will continue as normal. Thanks for your attention to this request. We apologize for any inconveniences.

Warning!!! Account owner that refuses to update his/her account after two weeks of receiving this warning will lose his or her account permanently.

Sincerely,
The Windows Live Hotmail
• Once compromised, the scammer can:
  • send messages to your contacts & thousands of other recipients
  • reset passwords to other accounts based on messages in your account (statements, newsletters) and password-reset-over-email feature of many online services

Bank Account Phishing

Dear valued customer of TrustedBank,

We have received 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/generatecustomerinfo.asp

Once you have done this, our fraud department will work to resolve this discrepancy. We are happy you have chosen us to do business with.

Thank you,

TrustedBank

Member FDIC © 2005 TrustedBank, Inc.
Demo

• Context Aware Phishing Attack Example (Indiana University)

Other targets
'Phishing 2.0'

- The ITS-ISO has observed an increase in phishing attempts trying to trick users into installing malware on their computers
- Phishing attempts appear targeted to recipients (spear phishing)
Recent ISO Case

- From: "Microsoft Windows Agent" <juser@kennesaw.edu>
  Date: Mon, 19 Oct 2009 07:17:34
  To: <juser@kennesaw.edu>
  Subject: Conficker.B Infection Alert

- Dear Microsoft Customer,
  - Starting 18/10/2009 the 'Conficker' worm began infecting Microsoft customers unusually rapidly. Microsoft has been advised by your Internet provider that your network is infected.
  - To counteract further spread we advise removing the infection using an antispyware program. We are supplying all affected Windows Users with a free system scan in order to clean any files infected by the virus.
  - Please install attached file to start the scan. The process takes under a minute and will prevent your files from being compromised. We appreciate your prompt cooperation.
  - Regards,
    Microsoft Windows Agent #2 (Hollis)
    Microsoft Windows Computer Safety Division
- Attachment: install.zip.exe

ITS-ISO Analysis

- Scam message originated off-campus and was able to bypass campus spam and virus filtering
- Contained self-extracting executable as attachment
- Attachment contained malware: a new variant of Trojan.FakeAV undetected by antivirus applications
Demo

- Testing a suspicious file on virscan.org

Similar Scams

- UPS Package Invoice
- IRS Unreported / Underreported Income
Protective Measures

- Make sure you have the latest operating system security updates
- Ensure your antivirus / anti-spyware / firewall application is up to date
- Check for & apply security patches for other applications: Java, Adobe Reader, Adobe Flash, etc.

Thank You

- Questions?