Ali Baba and the 40 Thieves
Protecting yourself in a hostile online world

Harvard Townsend
Kansas State University
Chief Information Security Officer
harv@ksu.edu

2009 IT Security Training Event
April 9, 2009
Fooling the 40 (thousand) Thieves
Agenda

- The Threats
- Definitions
- How to identify a scam
- Should I click on this?
- Protecting your eID password
- So you think your computer is compromised?
- Protecting your personal identity information
- Q&A
The Threats

It’s an increasingly hostile world online

- The times (threats) they are a changin’
- Identity theft
- Financial fraud/theft
- Physical theft (your laptop, USB drive)
- Information loss/theft (personal, institutional, passwords, acct info)
- Compromised computers used to send spam, host scam web sites, spread malware, steal data, launch denial of service attack, etc.

The user plays a key role in combating all these threats!
Vectors for attack

- Vulnerable operating system (i.e., Windows)
- Vulnerable applications
- Hackers scanning our network from outside or inside the campus network
- Stolen passwords
- USB flash drives
- Malicious web links, even sponsored ads at the top of a Google search
- Web links in an email
- Malicious Facebook ads
- Email attachments
- Extra goodies in P2P downloads
- Instant messaging
- Redirected DNS queries
- Hijacked duplicate web site
Real K-State Federal Credit Union web site

Fake K-State Federal Credit Union web site used in spear phishing scam

Introducing Stronger Security
We can identify you by checking the computer(s) that you are using to access our Web site. Typically you will access our Web site from one or two computers, such as your work and home machines. Either way, our Web site will remember your computer, preventing potential fraudsters from logging into your account even if they acquire or guess your Logon ID and password. Should you need to log in from a different computer, such as an Internet cafe, we will take additional steps to verify your identity, through a series of Challenge Questions you set up at the time of enrollment.

Christmas Savings CD
Definitions

- **Malware** – malicious software
  - *Virus, Worm, Trojan, etc.* - types of malware, specific definitions not that important now; “virus” sometimes used as a catch-all for malware
  - *Keylogger* – watches your keystrokes and intercepts data of interest; often sends it to the perpetrator. Typically looks for things like username/password, bank account info, credit card info
  - *Rootkit* – malware that tries to hide the fact that it compromised the computer. Think of it as stealth malware.

- **Spyware** – watches your online activity and sends information about you or your habits to others w/o your informed consent

- **Adware** – automatically displays ads on your computer, usually in annoying pop-ups

- **Scareware** – tries to trick you into buying something of little or no value using shock, anxiety or threats (like Anti-virus 2008/2009). Common tactic is to claim your computer is infected and you have to buy their software to clean it up.
Scareware examples

Warning!
Spyware detected on your computer!
Install an antivirus or spyware remover to clean your computer.

System Error!
Attention, Forensics! Some dangerous trojan horses detected in your system. Microsoft Windows XP files corrupted. This may lead to the destruction of important files in C:\WINDOWS. Download protection software now!
Click OK to download the antispyware. (Recommended)
Yes  No
Definitions

- **Phishing** – attempt to acquire sensitive information by posing as a legitimate entity in an electronic communication
- **Spear phishing** – phishing that targets a specific group
- **Social engineering** – manipulating or tricking people into divulging private information
- **Spam** – unsolicited or undesired bulk email/messages
Subject: KSU.EDU WEBMAIL ACCOUNT UPDATE
From: Help Desk <helpdesk@ksu.edu>
Reply-To: helpdesk-support@info.it
Date: 4/1/2009 2:54 PM
To: undisclosed-recipients <undisclosed-recipients;>

Attn: Faculty/Staff/Students,

This message is from ksue.edu IT Help Desk to all ksue.edu webmail account owners.

We noticed that webmail account has been compromised by spammers. It seems they have gained access to webmail accounts and have been using it for illegal internet activities.

The centre is currently performing maintenance and upgrading its database. We intend upgrading our Email Security Server for better online services.

You are to send us your account information immediately to enable us reset your account. A new password will be sent to you once this is done.

Send the information as follows:

* K-State eID:
* Password:
* Alternate email:

In order to ensure you do not experience service interruptions, please reply this email immediately and provide the following information above to prevent your account from being deactivated from our database.

Thank you for using our online services.

Webmail Administrator.
Definitions

- **Personal identity information (PII)** – information that can be used to uniquely identify an individual, like your name in conjunction with your SSN, driver’s license #, or credit card #

- **Identity theft** – fraud involving someone pretending to be someone else, usually for the purpose of stealing money or acquiring benefits

- **Financial fraud** – often the result of identity theft, where someone obtains money by posing as another person; examples include accessing an existing account or opening a new credit account with the stolen identity.
How to identify a scam

- Primarily focus on email, but are many other sources and types of online scams (aka “Internet fraud”) these days:
  - Web sites
  - Auction site fraud (misrepresent the product you’re bidding on, deliver damaged goods, never deliver, etc.)
  - Credit card fraud, bank/financial fraud, government documents fraud, medical services, phone or utilities fraud, etc.
  - Phone calls (I know... not “online”)
How to identify a scam

- General principles:
  - Neither IT support staff nor any legitimate business will EVER ask for your password in an email!!!
  - Use common sense and logic – if it’s too good to be true, it probably is.
  - **Think before you click** – many have fallen victim due to a hasty reply
  - Be paranoid
  - Don’t be timid about asking for help
How to identify a scam

- Characteristics of scam email
  - Poor grammar and spelling
  - Uses unfamiliar or inappropriate terms (like “send your account information to the MAIL CONTROL UNIT”)
  - It asks for private information like a password or account number
  - The message contains a link where the displayed address differs from the actual web address
  - It is unexpected (you weren’t expecting Joe to send you an attachment)
  - The “Reply-to:” or “From:” address is unfamiliar, or is not a ksu.edu or k-state.edu address
  - The message did not originate from a logical source (recent spear phishing scams coming from Nigeria, Mauritius, Lithuania)
  - Does not provide explicit contact information (name, address, phone #) for you to verify the communication
Let’s look at some examples

- Check IT Security Threats blog for examples of spear phishing scams: threats.itsecurity.k-state.edu

- Analysis of actual scams received by people at K-State
Can I click on this?

- Watch for displayed URL (web address) that does not match the actual displayed: http://update.microsoft.com/microsoftupdate actual: http://64.208.28.197/ldr.exe
- Avoid numeric IP addresses in the URL
- Watch for legitimate domain names embedded in an illegitimate one http://leogarciamusic.com/servicing.capitalone.com/c1/login.aspx/
- Beware of email supposedly from US companies with URLs that point to a non-US domain (Kyrgyzstan in example below)
  
  From: Capital One bank <cservice@capitalone.com>
  Actual URL: http://towernet.capitalonebank.com.mj.org.kg/onlineform/
Trend Micro Web Reputation Services is your friend
So are anti-phishing/malware features in Firefox and IE.
Evaluating a file you received

- Saving it to your desktop without opening it or executing it is usually safe
- Update Trend Micro OfficeScan and scan the file
- Submit to www.virustotal.com to be evaluated by 40 anti-virus products; here’s an example:
  
  virustotal.com/analisis/b299e2ac8871cd3e511db312d3f3e55d

- Contact the sender to verify they sent it
- Open it on an imaged computer or in a virtual machine (i.e., isolate its impact)
- Ignore or delete it if it’s not expected or important
Protecting your eID password

- **Never** share your eID password with ANYONE under any circumstances – K-State policy prohibits it: “eID passwords must not be shared under any circumstances.“
- Don’t let your browser or OS save it
- Don’t use it for any other account outside K-State
- Avoid using it in Internet Cafés and other public computers, if possible
- Use K-State VPN service to access K-State resources when possible
- Change your eID password when you get home after traveling as a precaution
Is your computer compromised?

Typical symptoms

- Internet stops working (we blocked it!)
- Slow, inconsistent performance
- Annoying, persistent pop-ups
- Pop-up message from Trend Micro OfficeScan (they may be annoying, but pay attention to these!)
- Some programs quit working or crash
- A new user account you did not create
- You can no longer login with your username+pw
- Hard drive active (light flickering) continually even when you’re not using it
- Anti-virus software quits working or won’t update
- Unusual programs running (seen in Task Manager)
What should you do if you think your computer is compromised?

- Stop using the computer so you don’t alter evidence
- Unplug the network cable
- **Leave the computer running!**
- Contact your IT support person immediately
- Contact the central IT security team (abuse@ksu.edu) and your SIRT rep – your IT support person can do this
- Critical question to ask – is there any confidential data stored on the computer?
  - Special incident handling procedures kick in if the computer has confidential data
  - State law (and ethics) may apply, requiring prompt investigation and notification of victims if personal identity information involved.
Protecting Your Personal Identity Information

- **Definition:** “information that can be used to uniquely identify an individual, like your name in conjunction with your SSN, driver’s license #, or credit card #”
- Don’t give out your SSN unless you absolutely have to
- Don’t read your SSN or account number out loud anywhere others can hear it; write it down on a piece of paper to give to the person instead of speaking it (get the paper back too!)
- Check your credit report three times per year
  - Entitled to one per year from each of the three credit reporting agencies; check different one every 4 months
  - [https://www.annualcreditreport.com](https://www.annualcreditreport.com)
Protecting Your Personal Identity Information

While traveling:
- ... overseas, always know where your passport is
  - Stow it securely on your person
  - Hide it in your hotel room or put it in a safe
- Beware of pick-pockets
- Conceal your valuables
- Pay with cash as much as possible (so you don’t have to use your credit card)
- Let your credit card companies know your travel destination and dates
- Beware of “ATM skimming” (device placed on ATM machine to steal your account info)
- Don’t let a vendor/server take your credit card out of your sight
What’s on your mind?