

IT Security Roundtable on recognizing scams and dealing with identity theft

Kansas State University

March 7, 2008

Harvard Townsend, IT Security Officer

Speaker Notes

1. Email scams sent last week to K-Staters

- Identify scam characteristics in two e-mails:
 - From “Ksu Team”
 - “Confirm Your E-mail Address”
- Both are classic “spear phishing” attempts
- Define phishing - attempt to criminally and fraudulently acquire sensitive information, such as usernames, passwords and credit card details, by masquerading as a trustworthy entity in an electronic communication. Trying to trick you into divulging private info.
- “Spear phishing” targets a specific population (e.g., only ksu.edu and k-state.edu e-mail addresses got the scam e-mail from the “Ksu Team”)

2. Other recent scams

- IRS scam (mouse over URL to show the difference in displayed and actual URL)
- Show them how to find country codes (<http://www.iana.org/root-whois/index.html>)
- Demonstrate clicking on Link and resulting Firefox warning; Thunderbird also warns of possible malicious links
- Often sites taken down fairly quickly, but not always (KSU FCU took weeks to go offline)
- WHOIS query to see owner of domain to see they are connected to the entity claiming to be sending the message (<http://www.networksolutions.com/whois/index.jsp>)
- Others prey on sympathies/compassion related to disasters – Katrina, Tsunami in Indian Ocean in 2004

3. General rules

- Apply logic – think before you click. Ask “does this make sense?”
- IT Support or a bank will never ask for password in an e-mail
- Call the alleged sender to verify
- Be cautious/suspicious
- Don’t ever reply – just validates your e-mail to spammers

4. If you mistakenly reply or click on a link

- Typically just clicking to visit a site won’t hurt you – don’t fill out info. Some links will auto-execute to exploit a vulnerability in a browser, or install malware. Rare, though.
- If you provided a password, go to source system and change pw immediately. Contact me so I can help determine if any systems were accessed
- If credit card info, notify police, call company, cancel account, check acct. statement for several months, run free credit report one month after incident
- If bank account info, call the police, call the bank and ask for advice on whether to close the account or just change the password and have them monitor it. Run free credit report one month afterwards
- If personal identity, notify police, place fraud alert, run credit report one month after incident to give time for the fraud to occur, file a complaint with the Federal Trade Commission at www.consumer.gov/idtheft.
- If driver’s license number or other govt-issued ID, contact the agency to determine how to invalidate old one and get a new one. Ask agency to “flag” your file to keep anyone else from getting a license or another identification document in your name.
- **Important to file a report with the police (aka Identity Theft Report)** - provides specific details of the identity theft, which entitles you to certain legal rights when it is provided to the three major credit reporting agencies or to companies where the thief misused your information. An Identity Theft Report can be used to permanently block fraudulent information that results from identity theft, such as accounts or addresses, from appearing on your credit report. It will also make sure these debts do not reappear on your credit reports.

Identity Theft Reports can prevent a company from continuing to collect debts that result from identity theft, or selling them to others for collection. An Identity Theft Report is also needed to place an extended fraud alert on your credit report.

- Notify me if it involves a K-State system or done by a K-Stater in the line of their work, or you just want advice.
- K-State police helpful as well.

5. Clues you've been victimized:

- Follow up with creditors if your bills don't arrive on time. A missing bill could mean an identity thief has taken over your account and changed your billing address to cover his tracks.
- Receiving credit cards that you didn't apply for;
- Being denied credit, or being offered less favorable credit terms, like a high interest rate, for no apparent reason; and
- Getting calls or letters from debt collectors or businesses about merchandise or services you didn't buy.
- Continue to read your financial account statements promptly and carefully every time, and to monitor your credit reports every few months the first year of the theft, and once a year thereafter

6. Identity theft

- Definition: catch-all term for crimes involving illegal usage of another individual's identity. FTC: identity theft occurs when someone uses your personally identifying information, like your name, Social Security number, or credit card number, without your permission, to commit fraud or other crimes.
- 9-10 million victims per year in the US alone
- Heard reports that FBI claims is fastest growing crime in US
- Identity = name + SSN + addr + DOB (think of the info needed to get a credit card)
- Show online credit card application form, like <https://app.firstusa.com/ICAppServlet?SPID=BBYM&PID=1166&CELL=6B01&AFFID=&CLICK=&CID=&PROMO=DF01>
- Senate Bill 196 defines it very specifically and requires notification of victims
- What can they do with your identity?
 - Most common thing is to open up a new credit account in your name
 - Sell on the black market

Credit card fraud:

- They may open new credit card accounts in your name. When they use the cards and don't pay the bills, the delinquent accounts appear on your credit report.
- They may change the billing address on your credit card so that you no longer receive bills, and then run up charges on your account. Because your bills are now sent to a different address, it may be some time before you realize there's a problem.

Phone or utilities fraud:

- They may open a new phone or wireless account in your name, or run up charges on your existing account.
- They may use your name to get utility services like electricity, heating, or cable TV.

Bank/finance fraud:

- They may create counterfeit checks using your name or account number.
- They may open a bank account in your name and write bad checks.
- They may clone your ATM or debit card and make electronic withdrawals your name, draining your accounts.
- They may take out a loan in your name.

Government documents fraud:

- They may get a driver's license or official ID card issued in your name but with their picture.
- They may use your name and Social Security number to get government benefits.
- They may file a fraudulent tax return using your information.

Other fraud:

- They may get a job using your Social Security number.

- They may rent a house or get medical services using your name.
- They may give your personal information to police during an arrest. If they don't show up for their court date, a warrant for arrest is issued in your name.
- <http://www.k-state.edu/infotech/security/topics/idtheft.html> for more info

7. Financial fraud

- Stolen credit card or bank account info; often considered “identity theft”; often stolen identity used to open an account to run up charges before you realize it.
- Credit card fraud alone – losses in the billions annually (\$51 billion in 2007, \$58 billion in 2006)
- Can run up a large bill quickly (friend in Rome - \$13,000 charged in 2 hours after pick-pocket theft; took him 4 months to get it cleared up)
- Big hassle to get it cleared (avg. 40-60 hours of your time)

8. Credit card vs. debit card

- Some recommend using credit card instead of debit card since the former has lower limits on your liability (\$50 by US law). Many credit card companies will even waive the \$50 liability and deduct the entire fraudulent charge (look for a “zero liability policy”)
- Debit card, they can withdraw cash from your account in series of ATM transactions (CapFed max per ATM transaction is \$500)
- Hackers focusing more on debit cards since stealing cash more attractive than purchasing goods
- Federal law with debit cards, liability is limited to \$50 only if customers notify their financial institution within two business days after realizing their card has been lost or stolen. After that, liability is capped at \$500 if suspicious activity is reported within 60 days of receiving a statement. Beyond 60 days, the sky's the limit.
- Often financial institutions do better than this with debit cards, though.

9. Fraud protection

FTC has nice description of the various products and services:

<http://www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idt05.shtm>

- Fraud alert
 - Done with the three national consumer credit reporting companies (TransUnion, Experian, Equifax)
 - File with one, they are required to report to the other two – call 800# phone
 - Alerts potential creditors that you might be victim of identity theft
 - They are supposed to use what the law calls “reasonable policies and procedures” to verify you’re your identity before issuing the credit
 - make it more difficult for someone to get credit in your name because it tells creditors to follow certain procedures to protect you
 - Doesn’t stop them from mis-using your current accounts
 - Also may delay your credit application
 - “Initial” only lasts 90 days;
 - can be renewed as needed
 - Can do this if *suspect* you are or will be a victim; do this when you lose your wallet or purse
 - entitles you to one free credit report from EACH of the credit reporting companies.
 - Does nothing to alert YOU if someone is able to open an account
 - “Extended” fraud alert = 7 years
 - Available to you if you can show you’re a victim of ID theft
 - Requires a police report (“Identity Theft Report”)
 - potential creditors **must** contact you in person, or by phone or some other method you have provided before they can issue credit in your name.
 - Entitled to two free credit reports from each company in 12 months
 - the consumer reporting companies must remove your name from marketing lists for pre-screened offers of credit for five years (less junk mail!!!!)

- Fee-based credit monitoring
 - Example from TransUnion: Free for 30 days, then \$11.95 per month
 - Unlimited access to your credit report
 - Alerts within 24 hrs of critical changes to your credit:
 - Fraudulent activity
 - New inquiries
 - New accounts
 - Late payments, etc.
 - \$25K ID theft insurance
 - Others simply charging you to do what you can do for free – fraud alert, credit freeze
 - Others help you recover from fraud; generally get limited power of attorney for you and deal with the creditors, reporting bureaus, etc. to get it cleaned up.
 - FTC cautions you to “read the fine print”. Some of these businesses are shady
- Credit freeze
 - Restricts access to your credit report
 - Potential creditors and certain other people or businesses can’t get access to it unless you lift the freeze temporarily or permanently; if they can’t see your credit rating, they generally won’t issue credit in your name.
 - Rules vary by state
 - Normally is a charge associated with it. Fee can be waived if prove you are a victim
 - Given a PIN to freeze/unfreeze (often \$10 a pop), and have to do it for each credit company
 - Can be a big hassle (and expense) since your credit information is accessed for MANY different purposes (loan, credit, mortgage, insurance, rental housing, employment, investment, license, cellphone purchase, utilities, Internet credit card transaction, etc.)
 - Jan. 11 IT Tuesday has an article on it:
 - <http://www.k-state.edu/infotech/news/tuesday/archive/2008/01-02.html#sectip>

10. Free annual credit report - <https://www.annualcreditreport.com/cra/index.jsp>

- Very good idea
- Federal law allows 1 free credit report from each credit bureau every 12 months
- Do one every 4 months from a different credit bureau for maximum coverage
- Beware of their attempt to sell you something (got to TransUnion.com –first thing you see is a “FREE” trial of a pay service)
- Also try to sell you access to your credit score (complex mathematical model that evaluates many types of information in a credit file. A credit score is used by a lender to help determine whether a person qualifies for a particular credit card, loan, or service. Most credit scores estimate the risk a company incurs by lending a person money or providing them with a service — specifically, the likelihood that the person will make payments on time in the next two to three years. Generally, the higher the score, the less risk the person represents.)
- What to look for:
 - Any new/unusual debt on existing accounts
 - Late payments on existing accounts
 - New accounts you don’t recognize
 - Regular inquiries – companies got your credit file; should be companies you did business with
 - Promotional inquiries – no concern other than it’s the source of much junk mail at home
 - Get rid of the pre-approved credit card mail: opt out for 5 years at www.optoutprescreen.com
 - Account review inquiries – watch for companies you did not contact
- There is a link on the report page to report inaccuracies

11. Repairing your credit

- Can be very time-consuming and difficult.
- Federal Trade Commission Credit Repair information at <http://www.ftc.gov/bcp/conline/pubs/credit/repair.htm>

Warnings from the FTC:

What about companies that claim they can improve my credit report for a fee?

The Federal Trade Commission (FTC) cautions consumers to be wary of companies that make claims regarding credit repair. These companies, commonly called credit clinics, don't do anything for consumers that consumers cannot do for themselves at little or no cost. Beware of any organization that offers to create a new identity and credit file for you. The FTC and state attorneys general have filed actions against those who pursue these fraudulent practices. Here are some warning signs that the FTC and others say consumers should look out for to determine if they might be dealing with a credit clinic:

- An organization that guarantees to remove late payments, bankruptcies, or similar information from a credit report
- An organization that charges a lot of money to repair credit
- A company that asks the consumer to write to the credit reporting company and repeatedly seek verification of the same credit account information in the file, month after month, even though the information has been determined to be correct
- An organization that is reluctant to give out their address or one that pushes you to make a decision immediately

12. How criminals steal your identity (stats from Javelin Strategy & Research Inc. study)

- 33% from physical theft of purse, wallet, credit cards, etc.
- 17% perpetrated by friend, relative, or in-home employee
- 14% due to Trojans, worms, phishing, or other malware and social engineering
- 7% data breaches

13. Prevention

- Get a shredder at home (financial stmts, credit card apps, anything with personal info)
- Teach yourself to recognize scams – think before you click!
- Protect your personal computer (AV software, personal firewall, patch OS and applications)
- Protect your passwords
- Refuse to give your SSN if it's not absolutely necessary
- Don't repeat your SSN in a public place – write it down and hand it to the clerk, then make them give it back to you so you can destroy it
- Don't provide personal info on the phone, through the mail, or on the Internet unless you're 100% sure of who you're dealing with
- Don't provide any personal or financial info in an Internet café or other public computer
 - Columbian man arrested in Florida for putting keyloggers on hotel business center and Internet lounge computers
- Use a VPN in public WiFi places
- Secure your home wireless
- Encrypt your laptop
- Run "spider" on your computers to discover all the SSNs and CC#s