Dissecting Phishing Scams

IT Security Training
April 13, 2011

Harvard Townsend
Chief Information Security Officer
harv@ksu.edu
Agenda

- Definitions with examples
- What’s the big deal?
- The numbers
- Phishing emails that were particularly effective
- How to recognize a phishing scam
- Defenses – are they working?
- Q&A
Definitions

- **Phishing** - attempt to acquire sensitive information, like bank account information or an account password, by posing as a legitimate entity in an electronic communication (example: an email that pretends to be from the IT Help Desk saying there’s a problem with email, so reply with your username and password to keep your email account active)

- **Spear phishing** – a phishing scam that targets a specific audience (the above example, but mentions Kansas State University and is sent to K-State email addresses)

- **Scareware** - tries to trick you into responding by using shock, anxiety or threats (“reply with your password now or we’ll shut down your email account tomorrow”)

- **Social engineering** - manipulating or tricking people into divulging private information (as opposed to using technical hacking techniques)
Phishing Example

Account Verification

From: "WEBMAIL TEAM" <upgrad@webmaster.com>
Reply To: upgrad@info.al

Dear webmail User,

To complete your Account Verification process, you are to reply this message and enter your ID and PASSWORD in the space provided (********), you are required to do this on receipt of this e-mail to prevent your Webmail Account from been de-activated and erased from our database.

Full Name:
Webmail User ID:
webmail Password:

Thank you for using our webmail service.

--
This message has been scanned for viruses and dangerous content by MailScanner, and is believed to be clean.
Subject: KSU.EDU WEBMAIL ACCOUNT UPDATE
From: Help Desk <helpdesk@k-state.edu>
Reply-To: helpdesk-support@ciudad.com.ar
Date: 7/5/2009 11:18 PM
To: undisclosed-recipients:<undisclosed-recipients>

Faculty/Staff/Students,

This message is from ksu.edu IT Help Desk to all ksu.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 center is currently performing maintenance and upgrading it's data base. 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.
Subject: KSU.EDU WEBMAIL ACCOUNT UPDATE

From: Help Desk <helpdesk@k-state.edu>

Reply-To: helpdesk-support@ciudad.com.ar

Date: 7/5/2009 11:18 PM

To: undisclosed-recipients <undisclosed-recipients;>

Att: Faculty/Staff/Students,

This message is from ksu.edu IT Help Desk to all ksu.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 center is currently performing maintenance and upgrading it's 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.
Scareware Example

K-State Webmail Account Maintenance

From: "K-State Web Mail Customer Care" <ksu@customercare.com>
Reply To: "customercare cc" <customercare.cc@hotmail.com>

April 6, 2011 9:05 AM

Dear 'K-State' E-mail User,

We are currently upgrading our database and all account need to be verified. To complete your account activation with us, you are required to reply to this message and enter correctly the information that is required from you.

Fill in your password in the space provided (*******). You are required to reply to this e-mail within the next 48 hours.

Failure to get back to us, your e-mail account will be de-activated from our database.

Full Name:
eID:
Password:

Thank you for using K-State WEB ACCESS Copyright 2011 © KSU Web Team.
Dear 'K-State' E-mail User,

We are currrently upgrading our database and all account need to be verified. To complete your account activation with us, you are required to reply to this message and enter correctly the information that is required from you.

Fill in your password in the space provided (*******) You are required to reply to this e-mail within the next 48 hours.

Failure to get back to us, your e-mail account will be de-activated from our database.

Full Name:
eID:
Password:

Thank you for using K-State WEB ACCESS Copyright 2011 © KSU Web Team.
Another Scareware Example

From: Hansen, Cindy [mailto:CindyHansen@mail.sunyjcc.edu]
Sent: Wednesday, March 30, 2011 11:10 AM
To: desk@admin.in.th
Subject: Upgrade Your Mailbox Today!

System Administrator in currently working to improve on the security of all
the Webmail Users as we periodically review certain Accounts which are
vulnerable to Unauthorised Access. We have noticed some unusual invalid
login attempts into your Webmail Account. Therefore your account has been
limited and may experience inability to send and receive new mail.

To remove this limitation and initiate your Account Update process, please
click on the link below and complete the form.

http://administratortechnicalsupport.yolasite.com/

Click on the link above (or copy and paste the URL address into your web
browser) to complete the form.

Localhost
Another Scareware Example

From: Hansen, Cindy [mailto:CindyHansen@mail.sunyjcc.edu]
Sent: Wednesday, March 30, 2011 11:10 AM
To: desk@admin.in.th
Subject: Upgrade Your Mailbox Today!

System Administrator is currently working to improve on the security of all the Webmail Users as we periodically review certain Accounts which are vulnerable to Unauthorised Access. We have noticed some unusual invalid login attempts into your Webmail Account. Therefore your account has been limited and may experience inability to send and receive new mail.

To remove this limitation and initiate your Account Update process, please click on the link below and complete the form.

http://administratortechnicalsupport.yolasite.com/

Click on the link above (or copy and paste the URL address into your web browser) to complete the form.

Localhost
Subject: Account Update.
From: Kansas State University <onlineupdate@k-state.edu>
Date: 1/23/2010 7:12 PM
To: undisclosed-recipients;

Dear User,

A scheduled maintenance has just been completed on our e-mail system. In order to keep this account active and protected, you will be required to immediately re-login. Kindly click on the "Login to My Account" link stated below:

Login to My Account

We apologize for any inconveniences caused.

Security Department,

E-mail Services.

Spear phishing scam received by K-Staters in January 2010
If you clicked on the link...
The malicious link in the email took you to an exact replica of K-State’s single sign-on web page, hosted on a server in the Netherlands, that will steal your eID and password if you enter it and click “Sign in”. Note the URL highlighted in red – “flushandfloose.nl”, which is obviously not k-state.edu
Fake SSO web page

Real SSO web page
Fake SSO web page – site *not* secure (http, not https) and hosted in the Netherlands (.nl)

Real SSO web page – note “https”
Fake SSO web page

Real SSO web page – Use the eID verification badge to validate
Result of clicking on eID verification badge on the fake SSO web site, or any site that is not authorized to use the eID and password.

This web site is not authorized to use K-State eIDs

Do NOT enter your K-State eID

Do not enter your K-State eID and password on the previous page. The owner and operator of that web site is not authorized to handle this sensitive information.

Entering your secret information may lead to the operator of that web site fraudulently using your information. If you have entered your eID and password at that web site previously, a good precaution would be to change your password now at the eID web site.

To report an unauthorized site requesting K-State eIDs, send e-mail to webmaster@k-state.edu with the site address.
Result of clicking on eID verification badge on a legitimate K-State web site that is authorized to use the eID and password for authentication
Real K-State Federal Credit Union website

Fake K-State Federal Credit Union website used in spear phishing scam
What’s the big deal?

- Criminals typically use stolen eID/password to login to K-State’s Webmail (from Nigeria!) and send thousands of spam emails to victims all over the world… with your name and email as the “From:” address
  - We’re contributing to the scourge of the Internet – spam!
  - You’re viewed as a spammer
  - K-State is viewed as a spammer
  - Email providers like Hotmail, Yahoo, Gmail, Comcast, etc. block ALL email from K-State, interfering with ability of faculty and staff to communicate with students and each other. MAJOR problem.

- Compromised Webmail account sometimes used to send the same phishing scam to others at K-State, so you may be indirectly responsible for other compromised accounts

- When detected, we disable your email and change your password, so you can’t get into anything with your eID

- If a criminal/hacker has your eID+password, **he can get into ANY K-State system that accepts your eID** (HRIS, iSIS, KSOL, eID Profile)
Not a good trend!!
K-State IT Security
Incidents in 2010

- Categories
  - 408 Spear phishing
  - 355 Spam source
  - 344 Unauthorized access
  - 103 Malicious code activity
  - 93 Policy violation
  - 83 DMCA violation
  - 23 Criminal activity/investigation
  - 10 Web/BBS defacement
  - 8 Reconnaissance activity
  - 3 Confidential data exposure
  - 1 Rogue server/service
  - 0 Un-patched vulnerability
  - 0 Denial of Service
  - 82 No incident

Mostly due to spear phishing scams (74% of all incidents!!)
A better trend!
(0.6 -> 0.9 -> 0.6 -> 0.7 per day)
First phishing scam detected at K-State on January 31, 2008
1,052 compromised eIDs since then and,
852 different phishing scams… that we know of
• 53 total phishing scam emails in 2011, year-to-date
  • 0.52 per day compared to 1.14 per day in 2010
• 25 compromised eIDs in 2011 YTD
  • 0.25 per day compared to 1.25 per day in 2010
• Last compromised eID on March 10!!... until this morning (April 13). 😞
Why the Improvement?

- Training/awareness efforts paying off?
- Added defense mechanisms working?
- Blocking malicious IP addresses at the campus border since Oct. 2010 (harder for hacker to login from Nigeria)?
- Aggressively blocking links/URLs in the form-based phishing scam emails (user prevented from getting to the web form that’s trying to steal their password)?
- Criminal(s) targeting us arrested?
- Rustock spam botnet shut down (probably not since it was taken down in March 2011)?
- Knock on wood…
Demographics of Phishing Scam Replies in 2010

- 390 Students (87% of total eIDs that replied to scams)
  - 95 Newly admitted, have not attended yet
  - 89 Freshmen
  - 55 Sophomore
  - 35 Junior
  - 54 Senior
  - 43 Graduate (31 Master’s, 12 PhD)
  - 6 Vet Med
  - 10 Alumni
  - 9 non-degree

- 26 Staff (24 current, 2 retired)

- 16 Faculty (6 current, 3 adjunct, 2 Instructor, 5 emeritus/retired)
  - 1 Post-Doc
  - 0 Senior administrators
  - 0 Other (like a sorority house mom)

- 13 Repeat offenders (retired HUMEC faculty wins the prize for replying 5 times; barely beat retired music faculty @ 4 replies)
Demographics of Phishing Scam Replies in 2010

- Gender
  - Female: 264 (58%)
  - Male: 192 (42%)
  - (60/40 last year)
Demographics of Phishing Scam Replies in 2010

- Students by academic college:
  - 34 – Agriculture
  - 88 – Arts & Sciences
  - 10 – Architecture
  - 28 – Business
  - 40 – Education
  - 34 – Engineering
  - 31 – Human Ecology
  - 5 – Technology & Aviation
  - 6 – Veterinary Medicine
  - 9 – Non-degree students
  - 20 – Undecided
Demographics of Phishing Scam Replies in 2010

<table>
<thead>
<tr>
<th>College</th>
<th>Count</th>
<th>Total in College</th>
<th>% of Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Education</td>
<td>40</td>
<td>1,422</td>
<td>2.81%</td>
</tr>
<tr>
<td>Human Ecology</td>
<td>31</td>
<td>2,026</td>
<td>1.53%</td>
</tr>
<tr>
<td>Architecture</td>
<td>10</td>
<td>663</td>
<td>1.51%</td>
</tr>
<tr>
<td>Agriculture</td>
<td>34</td>
<td>2,255</td>
<td>1.51%</td>
</tr>
<tr>
<td>Arts &amp; Sciences</td>
<td>88</td>
<td>6,687</td>
<td>1.32%</td>
</tr>
<tr>
<td>VetMed</td>
<td>6</td>
<td>462</td>
<td>1.30%</td>
</tr>
<tr>
<td>Engineering</td>
<td>34</td>
<td>2,998</td>
<td>1.13%</td>
</tr>
<tr>
<td>Business</td>
<td>28</td>
<td>2,493</td>
<td>1.12%</td>
</tr>
<tr>
<td>Technology/Salina</td>
<td>5</td>
<td>661</td>
<td>0.76%</td>
</tr>
</tbody>
</table>
More Phun Phishing Phacts

- In 2009, **79 of the 296 (27%) phishing scams were “successful”** (i.e., got replies with passwords) – no wonder the hackers don’t stop given this success rate!!

- Significant shift in the form of phishing since September 2010
  - Before, was 60-70% “reply to this email with your password”
  - Since September, 60+% are “click on this link and fill out the form”
Typical phishing form

- Hosted on compromised server
- Use of PHP Form Generator very common
Most Effective Spear Phishing Scam
Most Effective Spear Phishing Scam

Subject: KSU.EDU WEBMAIL ACCOUNT UPDATE

From: Help Desk <helpdesk@k-state.edu>

Reply-To: helpdesk-support@ciudad.com.ar

Date: 7/5/2009 11:18 PM

To: undisclosed-recipients <undisclosed-recipients;>

Attention Faculty/Staff/Students,

This message is from ksu.edu IT Help Desk to all ksu.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 center is currently performing maintenance and upgrading its data base. 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.
Subject: KSU.EDU WEBMAIL ACCOUNT UPDATE
From: Help Desk <helpdesk@k-state.edu>
Reply-To: helpdesk-support@ciudad.com.ar
Date: 7/5/2009 11:18 PM
To: undisclosed-recipients:<undisclosed-recipients;>

Attached: 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 center 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.
Most effective spear phishing scam

- At least 62 replied with password, 53 of which were used to send spam from K-State’s Webmail
- Arrived at a time when newly admitted freshmen were getting familiar with their K-State email – 37 of the 62 victims were newly-admitted freshmen
- Note characteristics that make it appear legitimate:
  - “From:” header realistic: "Help Desk" <helpdesk@k-state.edu>”
  - Subject uses familiar terms: “KSU.EDU WEBMAIL ACCOUNT UPDATE”
  - Message body also references realistic terms:
    - “IT Help Desk”, “Webmail”, “KSU.EDU”, “K-State”
  - Asks for “K-State eID” and password
  - Plausible story (accounts compromised by spammers!!)
Another effective spear phishing scam

This one also tricked 62 K-Staters into giving away their eID password

--- Forwarded Message -----
From: "Webmail Administrator" <asummers@k-state.edu>
To: undisclosed-recipients:;
Sent: Friday, October 30, 2009 6:56:46 AM GMT -06:00 US/Canada Central
Subject: webmail.ksu.edu Information Technology service

Attention webmail.ksu.edu Account holder,

This message is from the webmail.ksu.edu Information Technology service messaging center, to all webmail.ksu.edu e-mail account holders. All Mail hub systems will undergo regularly scheduled maintenance. Access to your mailbox via our mail portal will be unavailable for some period of time during this maintenance period.

We shall be carrying out service maintenance on our database and e-mail account center for better online services. We are deleting all unused e-mail accounts to create more space for new accounts.

In order to ensure you do not experience service interruptions/possible deactivation Please you must reply to this email immediately confirming your webmail.ksu.edu email account details below for confirmation/identification.

1. First Name & Last Name:
2. Full Login Email Address:
3. ID number:
4. Username & Password:
5. Confirm your Current Password:

Failure to do this may automatically render your e-mail account deactivated from our email/database/mailserver. To enable us upgrade your webmail.ksu.edu email account, please do reply to this mail.
Another effective spear phishing scam

Actually did come from a K-State email account... one that was compromised because the user gave away her eID password in another phishing scam!

--- Forwarded Message -----
From: "Webmail Administrator" <asummers@k-state.edu>
To: undisclosed-recipients:
Sent: Friday, October 30, 2009 6:56:46 AM GMT -06:00 US/Canada Central
Subject: webmail.ksu.edu Information Technology service

Attention webmail.ksu.edu Account holder,

This message is from the webmail.ksu.edu Information Technology service messaging center, to all webmail.ksu.edu e-mail account holders. All Mail hub systems will undergo regularly scheduled maintenance. Access to your mailbox via our mail portal will be unavailable for some period of time during this maintenance period.

We shall be carrying out service maintenance on our database and e-mail account center for better online services. We are deleting all unused e-mail accounts to create more space for new accounts.

In order to ensure you do not experience service interruptions/possible deactivation Please you must reply to this email immediately confirming your webmail.ksu.edu email account details below for confirmation/identification.

1. First Name & Last Name:
2. Full Login Email Address:
3. ID number:
4. Username & Password:
5. Confirm your Current Password:

Failure to do this may automatically render your e-mail account deactivated from our emaildatabase/mailserver. to enable us upgrade your webmail.ksu.edu email account, please do reply to this mail.
Even have form-based AND reply-to method in the same phishing scam email!

From: System Administrator [mailto:selena@selena.net.ua]
Sent: Friday, March 18, 2011 4:54 PM
Subject: Warning!!!

Dear Authorize Customer,

We are sorry to inform you that your online services are expired, and must be renewed immediately, if you intend to use these mailbox services in the future, and prevent any similarly situations you must take action at once!

To re-validate your mailbox please click the link below:

http://i12.admin/setup-account

Note: If the link above didn't work please send below information to the system administrator email address: accounts@xnmsn.cn

First Name:.............
Last Name:.............
E-mail:.................
Users Name:............
Password:.............

Thanks

System Administrator
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 – any email maintenance would be announced ahead of time (see the ITS status page); K-State also does not have an email quota
  - Think before you click – many have fallen victim due to a hasty reply
  - Be paranoid
  - Don’t be timid about asking for help from your IT support person or the IT Help Desk
How to identify a scam

- Characteristics of scam email
  - Poor grammar and spelling
  - The “Reply-to:” or “From:” address is unfamiliar, or is not a ksu.edu or k-state.edu address
  - 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, or tries to get you to click on a link that takes you to a web form that asks for the info
  - The message contains a link where the displayed address differs from the actual web address
  - Does not provide explicit contact information (name, address, and phone #, or a website) for you to verify the communication. Good example is spear phishing scam that tries to steal your eID password and is signed only by “Webmail administrator”
How to identify a scam

- Any email that says you’ve exceeded your email quota is a scam – **K-State’s email system has no quota** or limits on the space you use to store your email.

---

From: "System Administrator" <helpdesk@webmaster.com>
Sent: Friday, March 18, 2011 8:22:25 AM
Subject: Email Quota Limit

You have exceeded the storage limit on your mailbox.
You will not be able to send or receive new mail until you upgrade your email quota limit.
Click the below link and fill the form to upgrade your account.

http://latscape.com/formgen/use/Helpdesk/form1.html

System Administrator
192.168.0.11
Hackers very good at imitating legitimate email – will use official logos, some links in the email will work properly, but one link is malicious

Remember to use the eID verify badge on sites that ask for an eID password
Browser features – IE8

- Domain highlighting

```
http://static-host202-61-52-42.link.net.pk:85/IRS.gov/refunds.php
```

- SmartScreen filtering – block access to malicious sites and file downloads

![Image of website warning](image1.png)
![Image of download warning](image2.png)
Browser features - Firefox

- Anti-phishing and anti-malware protection – detects and blocks access to known malicious sites and downloads
Browser features - Firefox

- Instant Website ID – provides detailed identity information, if available, about the site:
Help from Trend Micro

- Web Reputation Services (WRS)
  - Blocks access to known disreputable sites, including those in phishing scams
  - Enabled in both Windows and Mac versions
  - K-State IT security team regularly reports new malicious links to Trend to add to the block list, especially those found in phishing scams
  - Will soon be able to add malicious URLs to our own “blacklist” in WRS so they’re blocked sooner
Trend Micro WRS is your friend
K-State’s Defenses Against Phishing Scams

- User training/awareness!
  - All 1,089 compromised eIDs could have been prevented by the user recognizing the scam and not responding!
  - Technology can’t intercept every scam email, nor stop users from clicking on a malicious link
  - “There’s no security patch for users!”
  - Now you know why we so strongly emphasize not giving away your password in the mandatory annual IT security training
K-State’s Defenses Against Phishing Scams

- User training/awareness continued
  - “Security-Alerts” email warnings to all users
  - IT security web site
  - “Safe email and web browsing” (ppt) seminars
  - Post examples on the IT security threats blog
  - Video+ads on the Jumbotron and radio at K-State football games in October 2011 (part of national cybersecurity awareness month)
  - Annual training events like the one today
  - Monthly security roundtables on a variety of security topics

- Teach yourself with Sonicwall’s “Phishing and Spam IQ Quiz” – www.sonicwall.com/phishing/
K-State’s Defenses Against Phishing Scams

- Process phishing scams as they come in
  - Notify ISPs hosting malicious URL/web form (to get it taken down), source of the phishing scam email (often a compromised email account elsewhere), and the email service provider of the reply-to address
  - Block malicious URL at the campus border
  - Submit malicious URL to Trend Micro to block in WRS
  - Submit reply-to address to “anti-phishing-email-reply” project
  - Post phishing emails to IT security threats blog

- Please send phishing scams you receive to abuse@ksu.edu with full headers
If you click on a malicious link in a phishing scam email that we know about, AND you are on campus, you are redirected to this page and prevented from going to the malicious site. Only works on campus.
K-State’s Defenses Against Phishing Scams

- Our email provider (Merit) is our partner in the battle
  - IronPort device rejects millions of spam messages a day, some of which are phishing scams
  - Many that get through are tagged as spam and put in Junk folders where they’re less likely to be noticed by the user (not necessarily the case for emails forwarded off campus)
  - Aggressive methods for quickly detecting compromised accounts (changes in account configuration, IP address making those changes, spam-like keywords added to the signature block, many sequential names added to AddressBook/Contacts, etc.)
  - There is no limit on the number of email messages an account can send, unlike our previous email hosting service (Yahoo)
  - Automatically lock student accounts at night that trigger these thresholds, lock faculty/staff after manual inspection

- After account locked, we reset the eID password so the hacker (and the legitimate user) can no longer use the account. Also remove configuration changes made by the hacker.

- IT Help Desk contacts the user for opportunistic “training” and help them change their password to reactivate the account
Things I’d like to do but haven’t done yet

- Required security training for students (coming this fall)
- Manage our own blacklist in Trend Micro Web Reputation Services (coming soon)
- Analyze log data to see if hackers are using stolen passwords to get into other K-State systems (coming soon)
- Block reply-to addresses in our email
- Block access to Zimbra email from known malicious IP addresses, esp. those from which hackers login with stolen passwords (block Nigeria!!)
- Greater consequences for those who give away their password?
- Send a fake phishing scam to see who is vulnerable? (NO!)
Conclusion

- Phishing has been a significant security concern for the last three years and consumed a huge amount of staff time.
- The training/awareness efforts and technological defenses seem to be paying off.
- But we cannot let down our guard.
- Social engineering is by far the most common way hackers infiltrate networks/systems now.
What’s on your mind?