

# Security Incidents at K-State

Harvard Townsend

Kansas State University

Chief Information Security Officer

*harv@ksu.edu*

2009 IT Security Training Event

October 5, 2009

October is



**NATIONAL  
CYBER SECURITY  
AWARENESS MONTH**

**Our Shared  
Responsibility**

[staysafeonline.org](http://staysafeonline.org)

# [ Agenda



- IT security incidents at K-State
- Interpretation of statistics
- Analysis of biggest problem of 2009 – spear phishing scams
- What are we going to do about it

# K-State IT Security Incidents in 2007



- 206 security incidents in 2007
  - 0.56 incidents per day
- Severity
  - 6 - High
  - 20 - Medium
  - 180 – Low
- Trend Micro Officescan stats:
  - 12,477 malware instances detected

# K-State IT Security Incidents in 2007



## ■ Categories

- 104 Malicious code activity
- 52 Spam source
- 27 Reconnaissance activity
- 18 Rogue server/service
- 12 Policy violation
- 10 Denial of Service
- 5 DMCA violation
- 5 Criminal activity/investigation
- 4 Unauthorized access
- 4 Web/BBS defacement
- 3 Confidential data exposure
- 0 Un-patched vulnerability
- 5 No incident

# K-State IT Security Incidents in 2008



- ~580 security incidents in 2008
  - 1.6 incidents per day
- Severity (531 recorded)
  - 2 - High
  - 20 - Medium
  - 499 - Low
  - 10 - NA
- ~150 spear phishing scams
  - 136 replies with eID/password
- Trend Micro Officescan stats lost in Control Manager upgrade

# K-State IT Security Incidents in 2008



## ■ Categories

- 180 Spam source
- 143 Spear phishing
- 91 Unauthorized access
- 84 Malicious code activity
- 66 Policy violation
- 56 DMCA violation
- 20 Reconnaissance activity
- 16 Web/BBS defacement
- 9 Criminal activity/investigation
- 4 Un-patched vulnerability
- 3 Confidential data exposure
- 3 Rogue server/service
- 1 Denial of Service
- 10 No incident

# K-State IT Security Incidents in 2009



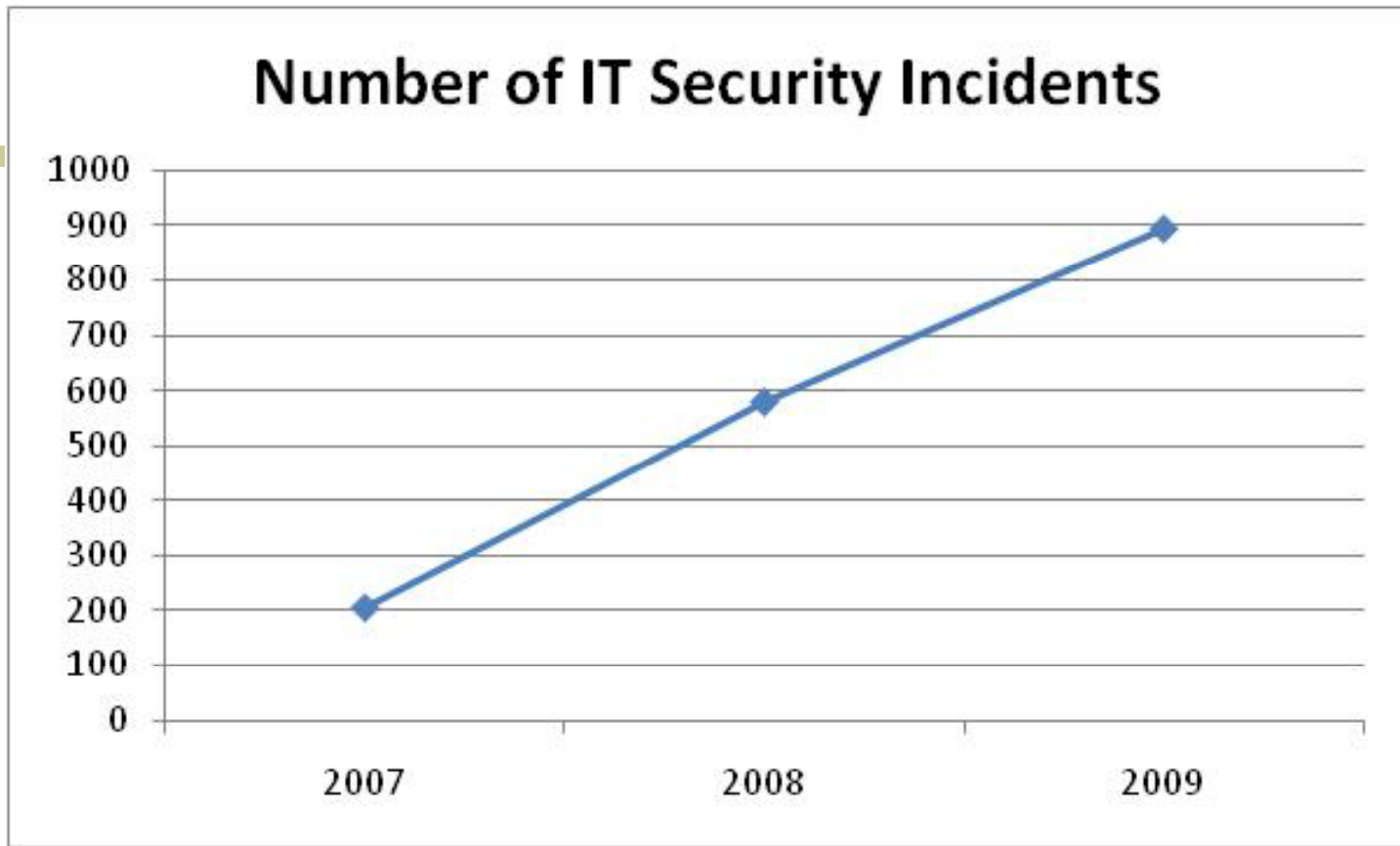
- 669 IT security incidents thus far in 2009
  - ~2.5 incidents per day
- Severity
  - 4 High
  - 7 Medium
  - 647 Low
  - 11 NA
- Trend Micro OfficeScan stats YTD:
  - 72,905 malware instances detected (97,500 extrapolated for full year!)
  - 13,033 spyware instances detected

# K-State IT Security Incidents in 2009



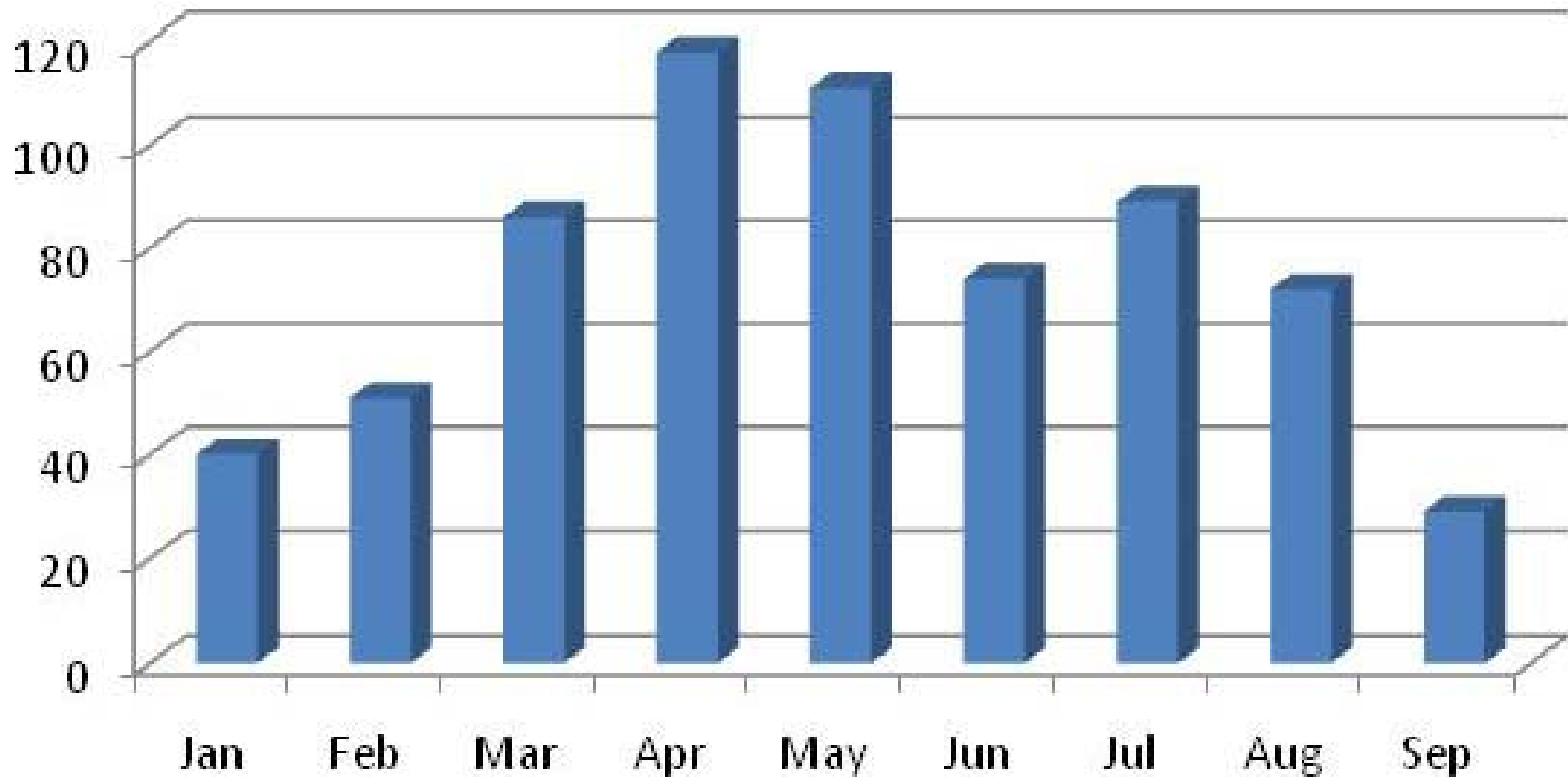
## ■ Categories

- 275 Unauthorized access
- 237 Spam source
- 223 Spear phishing
- 80 Malicious code activity
- 35 Policy violation
- 24 DMCA violation
- 13 Rogue server/service
- 11 Web/BBS defacement
- 7 Reconnaissance activity
- 6 Criminal activity/investigation
- 5 Confidential data exposure
- 1 Un-patched vulnerability
- 0 Denial of Service
- 11 No incident

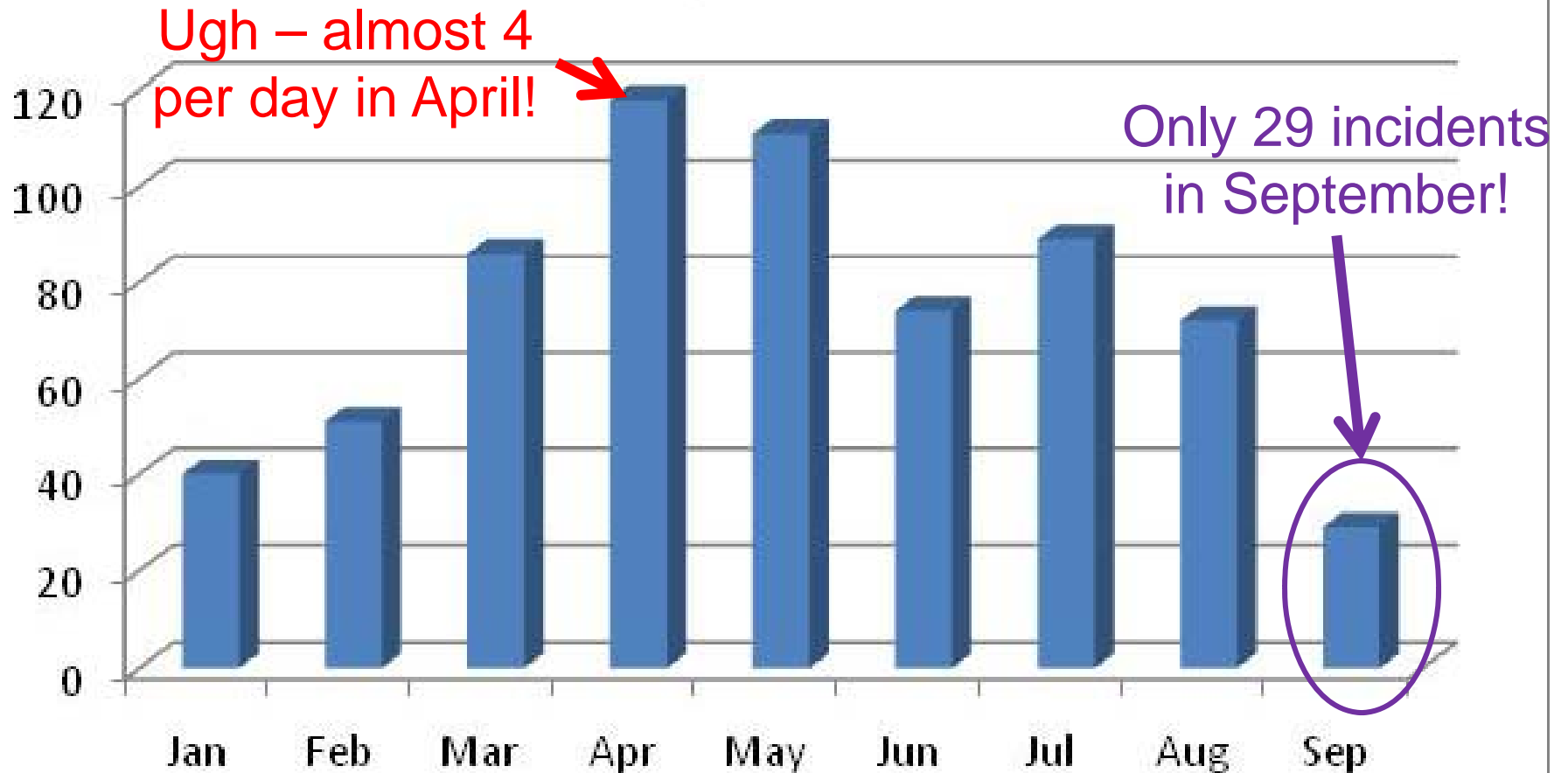


Not a good trend!!

## 2009 Security Incidents, YTD



## 2009 Security Incidents, YTD



Maybe September reflects a positive trend?!

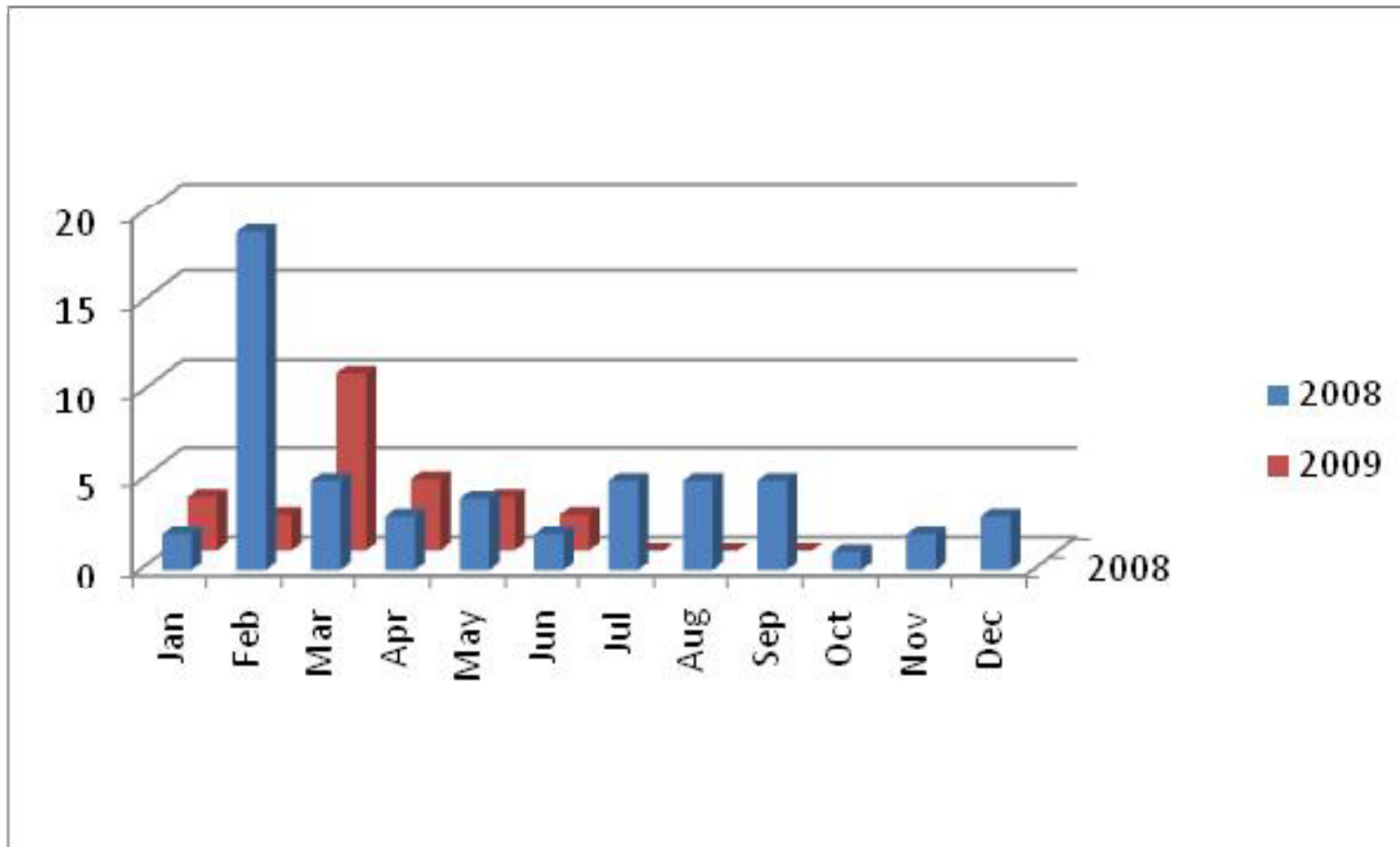
<i>Incident Categories</i>	<i>2007</i>	<i>%</i>	<i>2008</i>	<i>%</i>	<i>2009</i>	<i>%</i>
Confidential data exposure	3	1%	3	0%	5	1%
Criminal activity/investigation	5	2%	9	1%	6	1%
Denial of Service	10	4%	1	0%	0	0%
DMCA violation	5	2%	56	8%	24	3%
Malicious code activity	104	42%	84	12%	80	9%
Policy violation	12	5%	66	10%	35	4%
Reconnaissance activity	27	11%	20	3%	7	1%
Rogue server or service	18	7%	3	0%	13	1%
Spam source	52	21%	180	26%	237	26%
Spear phishing	NA	NA	143	21%	224	24%
Unauthorized access	4	2%	91	13%	275	30%
Un-patched vulnerability	0	0%	4	1%	1	0%
Web/BBS defacement	4	2%	16	2%	11	1%
No incident	5	2%	10	1%	11	1%
<b>Total</b>	<b>249</b>		<b>686</b>		<b>929</b>	
<b>Individual incidents</b>	<b>206</b>		<b>580</b>		<b>670</b>	
	<b>Extrapolated to full year:</b>				<b>894</b>	

# Observations 2007-2009



- **The threats are real and happening to K-State systems regularly**
- Increasing frequency of incidents (200 – 580 – ~900) a troubling trend
- 2007 was the year of botnets
- 2008 was the year of spam
- 2009 is the year of spear phishing... and spam
- Incidents involving confidential data remained about the same (which is NOT good – needs to be zero!)
- DoS less of an issue these days
- Dramatic increase in DMCA notices... but none thus far in fall 2009 after concerted education effort
- Reduction in “Reconnaissance activity” probably due to change in how malware spreads; is now more by user clicking on malicious links on a web page or in an email rather than through scanning the network for vulnerable computers
- Spam consistently a problem
- Had to create a new category in 2008 (spear phishing)
- Hijacking web sites, posting porn/drug ads on web sites a growing problem

# DMCA Copyright Infringement Cases



# [ Biggest Headache ]



- Spear phishing scams trying to steal eID passwords to use in Webmail to send spam
- The stats:
  - First appeared January 31, 2008
  - 143 in 2008, **227 known versions thus far in 2009**
  - 136 replied with their password in 2008, **314 thus far in 2009!!**
  - **264 compromised eIDs used to login to Webmail and send spam thus far in 2009**
    - 134 in 5 months prior to Zimbra, 130 in 4 months since the switch
- The headache:
  - Time-consuming for IT staff
  - Results in K-State being placed on spam block lists by major ISPs
  - Contribute to the worldwide scourge of spam
- Good example of “insider” or the user being a big part of the security problem. Also good example of effective social engineering

# Demographics of Scam Replies in 2009 YTD



- 276 Students
  - 97 Newly admitted, have not attended yet
  - 37 Freshmen
  - 36 Sophomore
  - 19 Junior
  - 44 Senior
  - 28 Graduate (17 Master's, 11 PhD) } They should know better!
  - 1 Vet Med
  - 3 Alumni
  - 11 non-degree
- 16 Staff (14 current, 2 retired)
- 17 Faculty (8 current, 3 adjunct, 6 emeritus/retired)
- 2 Senior administrators
- 3 Other (like a sorority house mom)
- 8 Repeat offenders (sophomores win the prize here w/ 4)

# Demographics of Scam Replies in 2009 YTD

- Students by academic college:
  - 31 – Agriculture
  - 62 – Arts & Sciences
  - 3 – Architecture
  - 13 – Business
  - 20 – Education
  - 18 – Engineering
  - 19 – Human Ecology
  - 8 – Technology & Aviation /Salina
  - 1 – Veterinary Medicine



# Most Effective Spear Phishing Scam



**Subject:** KSU.EDU WEBMAIL ACCOUNT UPDATE  
**From:** [Help Desk <helpdesk@k-state.edu>](mailto:helpdesk@k-state.edu)  
**Reply-To:** [helpdesk-support@ciudad.com.ar](mailto:helpdesk-support@ciudad.com.ar)  
**Date:** 7/5/2009 11:18 PM  
**To:** [undisclosed-recipients <undisclosed-recipients::>](mailto:undisclosed-recipients@ciudad.com.ar)

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.

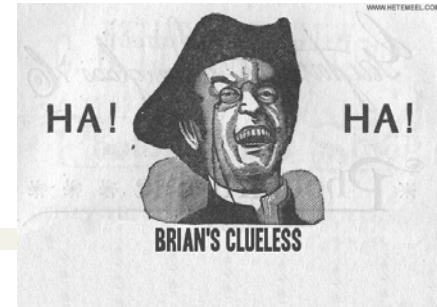
Webmail Administrator.

# 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:
  - "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!!)

# Most effective spear phishing scam



- Challenges with this scam:
  - ISP of reply-to address unresponsive in disabling account (in Argentina!)
  - Sent multiple times over the summer with slight variations
  - Couldn't block source IP of hacker since is now logging into Zimbra/Yahoo servers, not K-State's, plus they login from multiple compromised sources
  - Zimbra would not block replies to the reply-to address (like we used to do)
  - Zimbra anti-spam/anti-malware filters ineffective

# Security Strategy for 2009



- Spear phishing
  - Seems to have slowed down this fall
  - Optimistic that new hosting service for Zimbra will give us more options
- Education campaign for P2P file sharing required by Higher Ed Opportunity Act of 2008 has helped
  - Annual disclosure to inform students about illegal sharing of copyrighted materials
  - “Effectively combat” the unauthorized distribution of copyrighted material.
  - “to the extent practicable,” offer alternatives to illegal file sharing
- Adding another person to the security team
- Expand vulnerability scanning
- Enhance intrusion detection, VPN, and firewall services<sub>21</sub>

# [ Security Strategy for 2009 ]



- Policy, policy, and more policy
  - Data classification and security
  - Incident reporting and response
  - Media sanitization and security
  - Audit-driven policies:
    - Physical and environmental security
    - Access controls
    - System development and maintenance
    - Security Communications and Operations

# Continue Strengthening Protection of SSNs



- Sweep web sites
- SSN awareness campaign
  - Discover SSNs
  - Get rid of files no longer needed
  - Properly protect those that are needed
- Make Spider (tool that finds SSNs, credit card #s) more widely available
- Implement data classification security standards

# Can't Rely Solely on AV Tools

- Characteristics of malware make pattern-based antivirus defense inadequate
  - Malware changes rapidly
  - 50,000 new forms DAILY!
  - Can spread around the world in a matter of hours
- Hackers disable AV software

# [ More Holistic Approach ]



- AV software still has value
  - Use Web Reputation Services and other tools being added
- Strengthen personal firewalls
- Accounts w/o admin privileges
- Promote standard security configurations
- Continue user awareness

# [ What's on your mind? ]

