Online Security for the University of Alaska System
Prepared for the University of Alaska Board of Regents

June, 2009

Steve Smith
Chief Information Technology Officer
University of Alaska

UA Online Security Data Snapshot

Figure 1

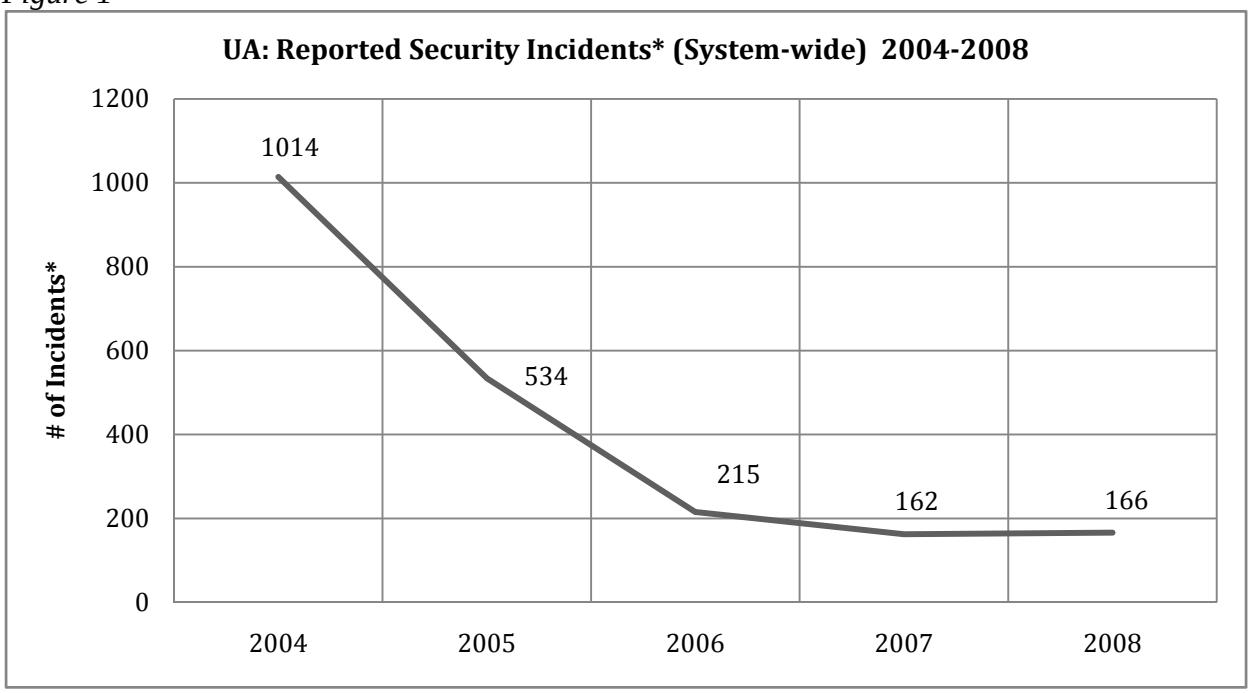
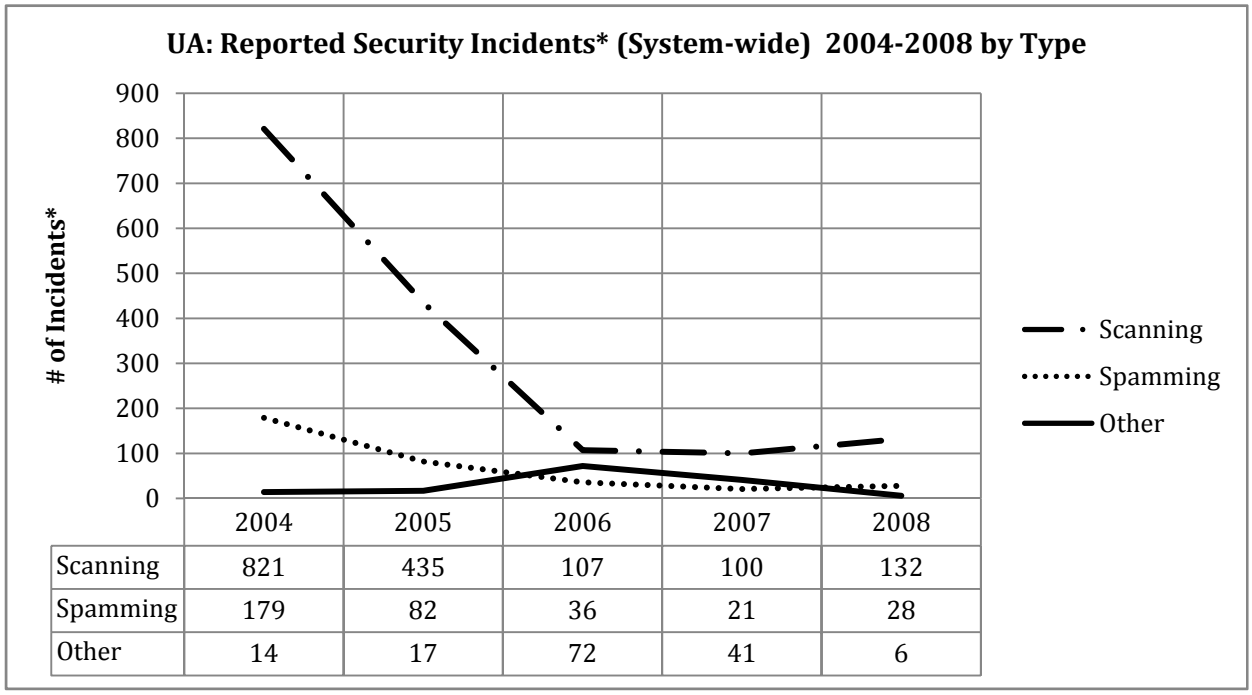


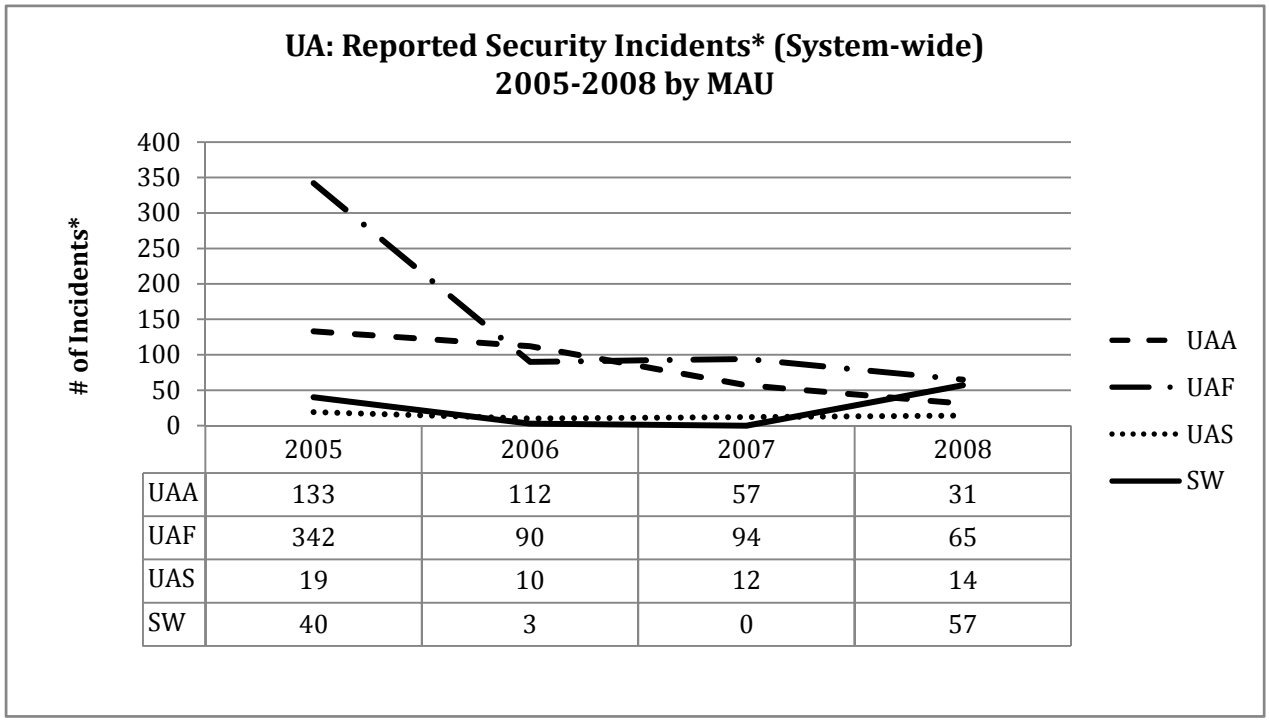
Figure 2



	2004	2005	2006	2007	2008
Scanning	821	435	107	100	132
Spamming	179	82	36	21	28
Other	14	17	72	41	6

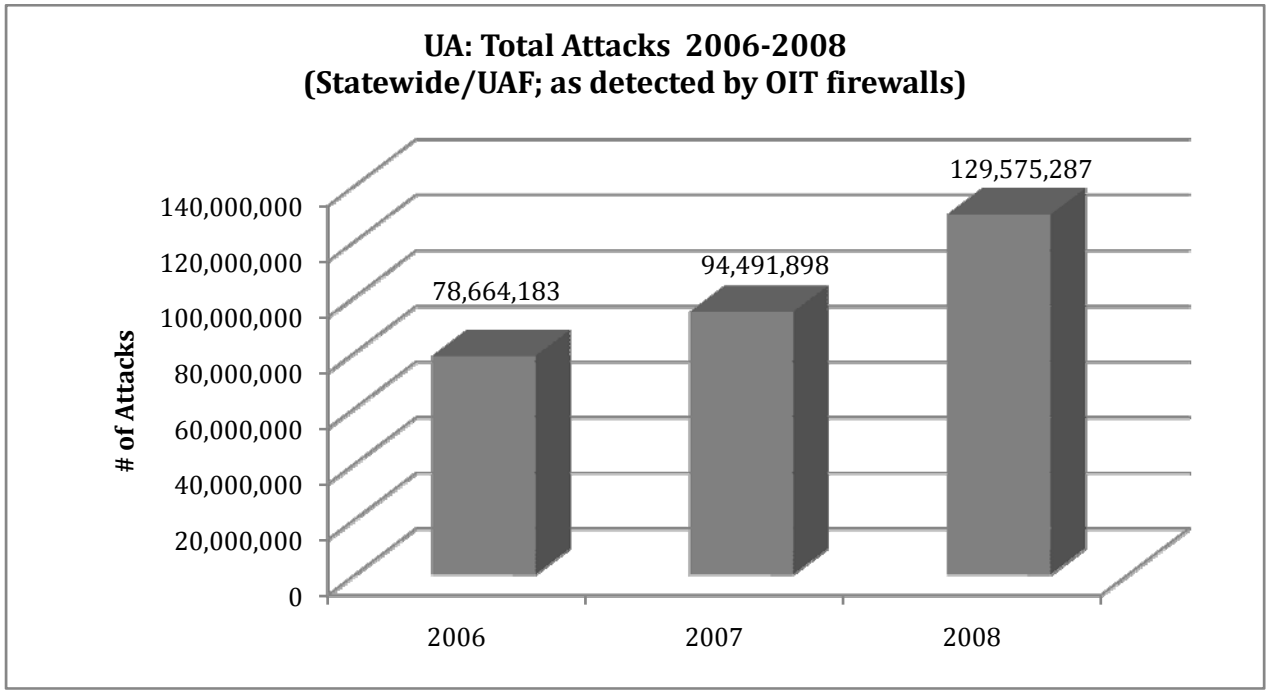
*An "Incident" is the compromise of a unique machine

Figure 3



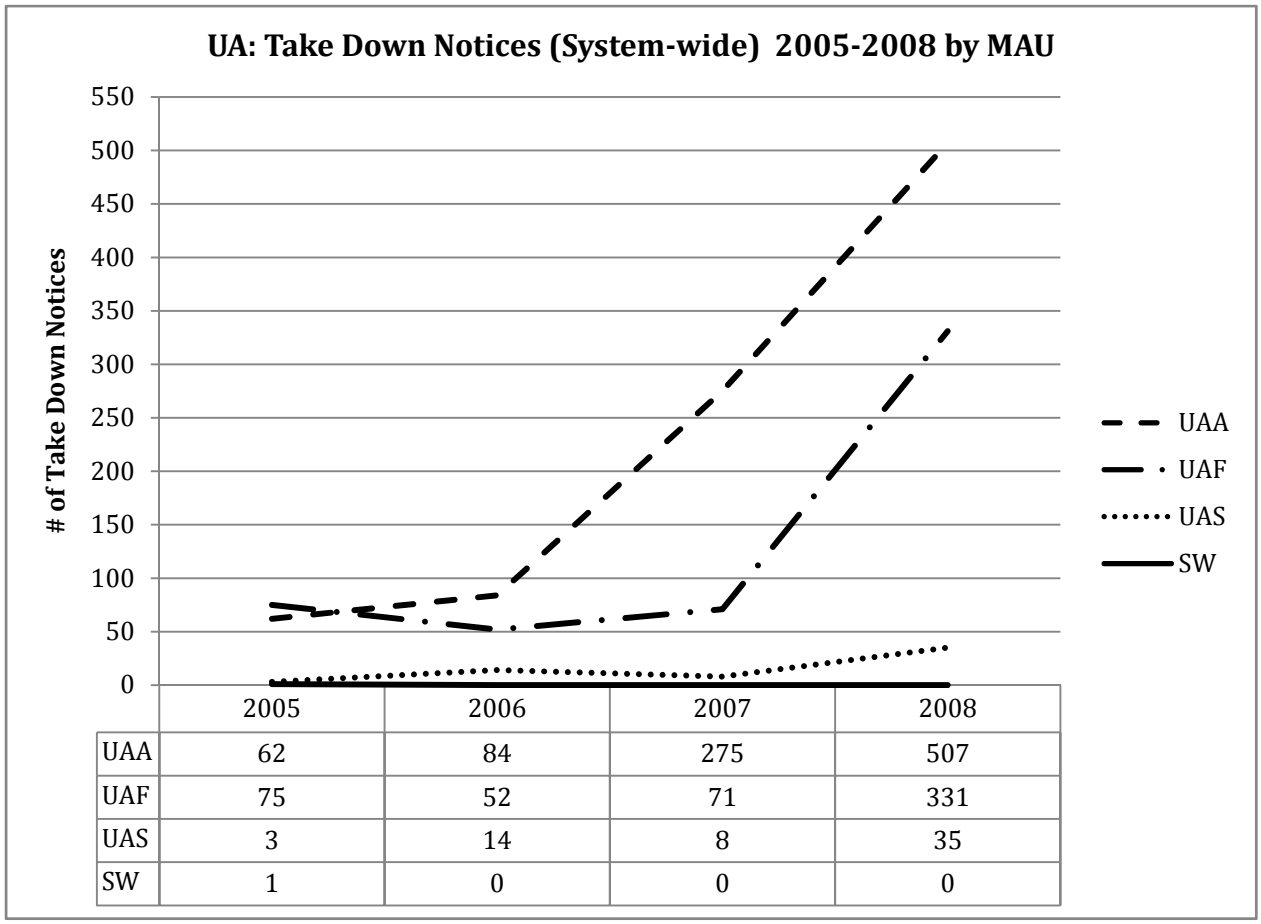
	2005	2006	2007	2008
UAA	133	112	57	31
UAF	342	90	94	65
UAS	19	10	12	14
SW	40	3	0	57

Figure 4



*An "Incident" is the compromise of a unique machine

Figure 5



	2005	2006	2007	2008
UAA	62	84	275	507
UAF	75	52	71	331
UAS	3	14	8	35
SW	1	0	0	0

A **Take Down Notice** is a request to stop distribution of suspected copyrighted materials. This is generally due to use of file sharing applications.

A **Preservation Notice** is a request to preserve data that might identify the user of a machine at the time of a suspected copyright violation.

An **Early Settlement Letter (ESL)** is a request sent to the University with the request to pass it on to the user of a specific identified Internet address (IP address) to settle with the RIAA for a fee to avoid litigation over the distribution of suspected copyrighted material.

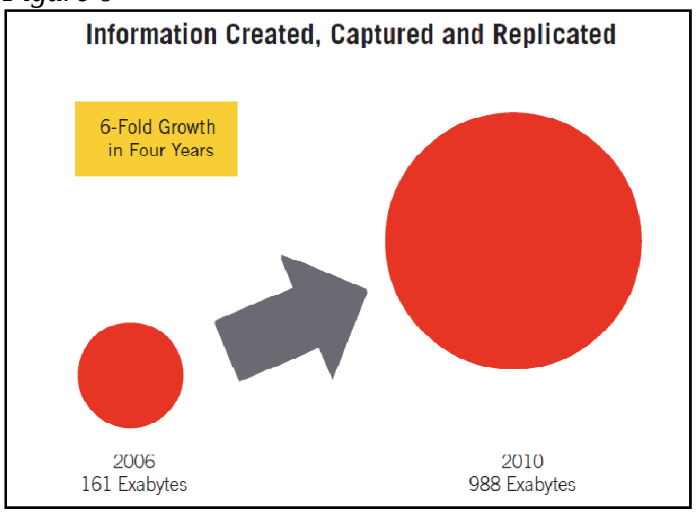
Breakdown of Copyright-Related Notices/Letters received by UA (Systemwide)

	2005	**2006**	**2007**	**2008**
Take Down Notices	141	150	354	873
Preservation Notices	0	0	5	2
Early Settlement Letters	0	0	0	12

Security Context

There is an explosion of digital content.

Figure 6[1]



Security becomes more complex as use of mobile devices and integration of applications (voice, video, data; from home to business to social networking) increases.

The mobile device will be the primary connection tool to the internet for most people in the world in 2020.

The transparency of people and organizations will increase, but that will not necessarily yield more personal integrity, social tolerance, or forgiveness.

Voice recognition and touch user-interfaces with the internet will be more prevalent and accepted by 2020.

Those working to enforce intellectual property law and copyright protection will remain in a continuing arms race, with the crackers who will find ways to copy and share content without payment.

The divisions between personal time and work time and between physical and virtual reality will be further erased for everyone who is connected, and the results will be mixed in their impact on basic social relations.

Next-generation engineering of the network to improve the current internet architecture is more likely than an effort to rebuild the architecture from scratch.[2]

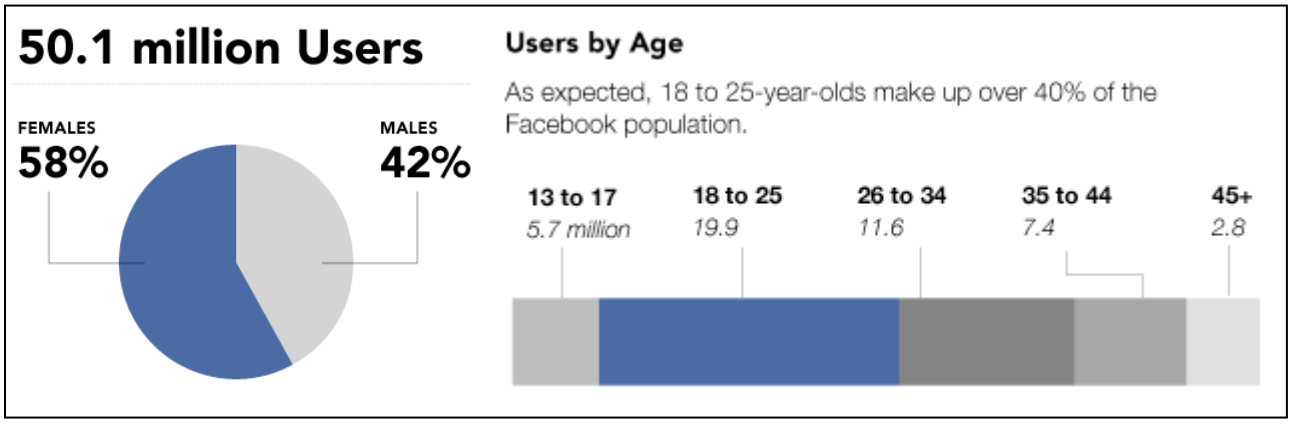
---

[1] From IDC "The Expanding Digital Universe" March 2007. http://www.emc.com/collateral/analyst-reports/diverse-exploding-digital-universe.pdf

[2] From the Pew Internet & American Life Project; "The Future of the Internet III" December 14, 2008 by *by Lee Rainie, Janna Anderson.*

Facebook was started by students at Harvard in 2004. It spread across U.S. universities. It is now open to anyone and has over **50 million users in the United States and 200 million active users worldwide**. It is currently the largest social network application.

Figure 7[3]



Twitter, a social network short messaging service application began in 2006 and has had a growth rate estimated at **1382%** and roughly 6 million monthly visitors. Like most social network sites, it is free.

As the user population and the uses grow so do malicious attacks and security threats.

> More than 97 percent of e-mail messages sent over the Internet are unwanted: they have malicious attachments or are phishing attacks or spam.[4]

[3] Facebook Statistics from Flowing Data http://projects.flowingdata.com/facebook/.
[4] From Microsoft Security Intelligence Report volume 6 (July through December 2008).

Figure 8[5]

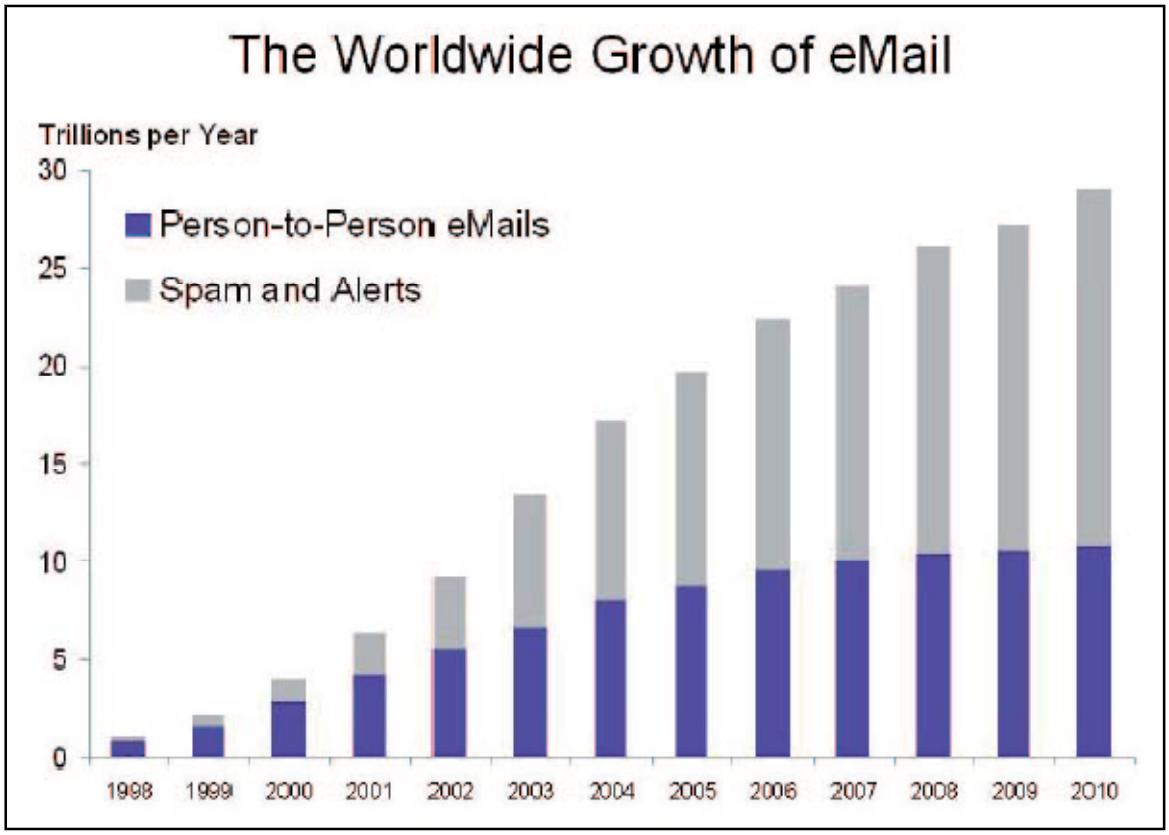
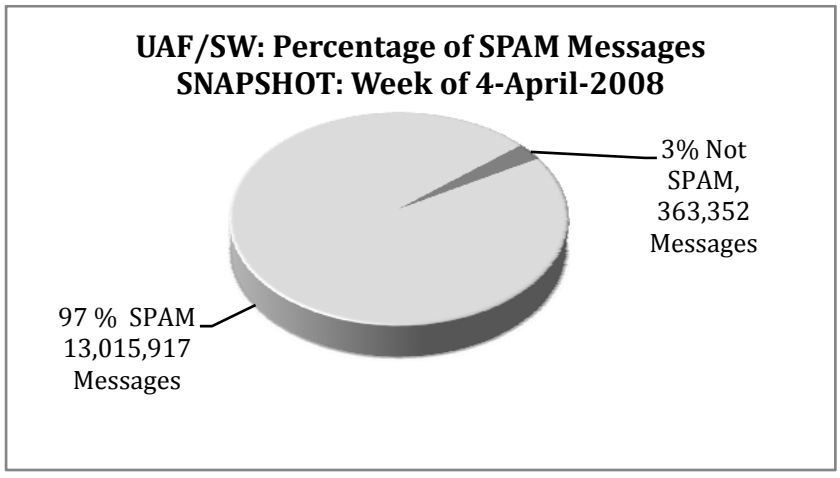


Figure 9



[5] From IDC "The Expanding Digital Universe" March 2007. http://www.emc.com/collateral/analyst-reports/diverse-exploding-digital-universe.pdf

Figure 10

Example of EMAIL phishing spam

To: <helpdesk@uaf.edu>
Subject: eMAIL ACCOUNT MAINTENANCE !!!
Reply-To: info_supportteam@ubbi.com

We are currently carrying-out a mentainace process to your UAF.EDU account, to complete this process you must reply to this email immediately, and enter your User Name here (_____) And Password here(_____) if you are the rightful owner of this account.

Changing Legal and Regulatory Environment

Changes in the law in response to the growing complexity of technology place more burdens on businesses and institutions to manage security and protect personal information.

- CFAA (Computer Fraud and Abuse Act)
- CIPA (Children's Internet Protection Act)
- CISP (Visa Cardholder Information Security Program)
- FERPA (Family Educational Rights and Privacy Act) – New Regulations & Rules concerning student information.
- GLBA (Gramm-Leach Billey Act)
- HB 65 (Alaska House Bill 65) –"*Relating to breaches of security involving personal information, credit report and credit score security freezes, protection of social security numbers, care of records, disposal of records, identity theft, credit cards, and debit cards, disclosure of the names and addresses of permanent fund dividend applicants, and to the jurisdiction of the office of administrative hearings;"*
- HEOA (Higher Education Opportunity Act) – New Rules on File Sharing in process.
- HIPAA (Health Insurance Portability and Accountability Act)
- PA-DSS (Payment Application Data Security Standard)
- PCI DSS (Payment Card Industry Data Security Standard)

- Red Flags Rule – Implements FTC Fair and Accurate Credit Transactions Act of 2003 concerning identity theft.

- Sarbanes-Oxley Act of 2002 (Public Company Accounting Reform and Investor Protection Act)

How the University of Alaska is Responding to Online Security Issues

- Policy and Regulation: Chapter 02.07 Information Resources, in place since 2000.

- UA CIRT (Computer Incident Response Team) is a system wide group of computer and network security staff who handle internal and external online security incidents.

- UAF Advanced System Security Education, Research, and Training Center (ASSERT) designated as a Center of Excellence in Information Assurance Education.

- UAA State of Alaska Election Security Project, in conjunction with Lt. Governor.

- System-wide External Security Review: completed in 2008 with remediation and internal review continuing. The next external review is planned for 2011.

- A Chief Records Officer position was created in 2007.

- All MAUs are reallocating or seeking resources to add staff and support to security.

Attachment 1
University of Alaska Information Resource Abuse Incident Report

Date: May 11, 2009

MAU: UAF

Incident Date/Time: 10 May 2009 00:39:34 GMT

Complaint received Date/Time: 11 May 2009 07:19:12 AKDT (GMT -0800)

Incident Type: [X]Copyright Infringement [ ]UCE [ ]Other

UA Case ID: [########-###]
CH Case ID: ###-########

Case Status: [X]Open/Pending Investigation [ ]Closed

Source IP Address: ###.###.##.###
Source Hostname: None

DESCRIPTION:

The above referenced host may be distributing copyright materials.
UAF Abuse Response Team please investigate and report.

1. Investigate the allegation
2. Take appropriate measures in accordance with University Regulations and UAF Rules & Procedures pertaining to copyright infringement.
3. Report back to shccc@email.alaska.edu measures taken excluding any information protected by FERPA, other Federal, State & local statutes. (Use check lists below)

RESOLUTION:

[X] Notified copyright@alaska.edu by: Chirk Chu on 05/11/09
[X] Notified abuse@uaf.edu by: Chirk Chu on 05/11/09
[X] Acknowledged receipt of complaint by: Chirk Chu on 05/11/09
[X] bsa@copyright-compliance.com

[ ] Identified owner of the system specified in the complaint
[ ] Unable to identify owner
by:
date:

[ ] Notified violator or supervisor of the violator of the infringement claim
by:
date:

[ ] Informed violator the University of Alaska's position on copyright, http://www.alaska.edu/active/level2/copyright.xml
by:
date:

[ ] Network access/account disabled
by:
date:

[ ] Verified the allegation to be:
[ ]TRUE
[ ]FALSE
verified by:
date:

[ ] Infringing materials removed
by:
date:

[ ] Offending system compromised; owner not involved; all infringing materials and malwares removed; system patched and restored
by:
date:

[ ] Other actions (please specify) taken
by:
date:

[ ] Responded to the complainant
by:
date:

NOTIFICATIONS:

Date: Mon, 11 May 2009 07:19:12 -0800
From: bsa-no-reply2@copyright-compliance.com
Subject: Copyright Infringement Notice ID: 197-5502542

11 May 2009 15:17:37 GMT

University of Alaska - Fairbanks

RE: Unauthorized Distribution of the following copyrighted computer program(s):

Dear Sir/Madam:

The Business Software Alliance (BSA) has determined that the above connection, which appears to be using an Internet account under your control, is using a P2P network seen below to offer unlicensed copies of copyrighted computer programs published by the BSA's member companies.

Evidentiary Information:
Notice ID: #######
Asset: Adobe Photoshop
Protocol: BitTorrent
IP Address: ###.###.##.###
DNS:
File Name: Adobe Photoshop CS3 Extended
File Size: 595998362

Timestamp: 10 May 2009 00:39:34 GMT
Last Seen Date: 10 May 2009 00:39:34 GMT
Username (if available):
Port ID: #####

The above computer program(s) is/are being made available for copying, through downloading, at the above location without authorization from the copyright
owner(s).

Based upon BSA's representation of the copyright owners in anti-piracy matters, we have a good faith belief that none of the materials or activities listed above have been authorized by the rightholders, their agents, or the law. BSA represents that the information in this notification is accurate and states, under penalty of perjury, that it is authorized to act in this matter on behalf of the copyright owners listed above.

We are giving notice of these activities pursuant to Section 512 of Title 17 of the U.S. Code (as enacted by the 'Online Copyright Infringement Liability Limitation Act'). We expect that you will take expeditious action to remove or disable access to the materials described above, and thereby prevent the illegal reproduction and distribution of pirated software via your company's network. As you know, illegal on-line activities can result in 50 million people on the Internet accessing and downloading a copyrighted product worldwide without authorization - a highly damaging activity for the copyright holder.

We appreciate your cooperation in this matter. Please advise us regarding what actions you take.

Please include the following Notice ID in any response you send:
###-#######

Please respond indicating the actions you have taken to resolve this matter. The provided link has been assigned to this matter [link removed]

For email correspondence, please reference the above Notice ID in the subject line
mailto:bsa@copyright-compliance.com

Yours sincerely,

Internet Enforcement Team
Business Software Alliance
1150 18th St NW Suite 700
Washington, DC 20036
URL: http://www.bsa.org
E-mail: bsa@copyright-compliance.com
1-888-667-4722

Attachment 2
Glossary of Common Information Security Related Terms[6]

Botnet is a jargon term for a collection of software robots, or bots, that run autonomously and automatically. The term is often associated with malicious software but it can also refer to the network of computers using distributed computing software.

A **denial-of-service attack** (**DoS attack**) or **distributed denial-of-service attack** (**DDoS attack**) is an attempt to make a computer resource unavailable to its intended users.

E-mail spoofing is a term used to describe fraudulent e-mail activity in which the sender address and other parts of the e-mail header are altered to appear as though the e-mail originated from a different source

File sharing is the practice of sharing digital information, such as music and video files, often in violation of copyright laws. It includes both the manual sharing of files using removable media and the use of peer-to-peer computer networks to allow direct access download.

Malware, a portmanteau from the words **mal**icious and soft**ware**, is software designed to infiltrate or damage a computer system without the owner's informed consent.

A **packet sniffer** is an application that captures data packets, which can be used to capture passwords and other data in transit over the network.

A **peer-to-peer** (or **P2P**) computer network uses diverse connectivity between participants in a network and the cumulative bandwidth of network participants rather than conventional centralized resources where a relatively low number of servers provide the core value to a service or application. P2P networks are typically used for connecting nodes via largely *ad hoc* connections. Such networks are useful for many purposes.

Sharing content files (see file sharing) containing audio, video, data or anything in digital format is very common, and real time data, such as telephony traffic, is also passed using P2P technology.

Phishing is the criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication.

Spam is the abuse of electronic messaging systems (including most broadcast mediums, digital delivery systems) to send unsolicited bulk messages indiscriminately.

In the context of network security, a **spoofing attack** is a situation in which one person or program successfully masquerades as another by falsifying data and thereby gaining an illegitimate advantage.

[6] Definitions from Wikipedia http://en.wikipedia.org/

Spyware is computer software that is installed surreptitiously on a personal computer to collect information about a user, their computer or browsing habits without the user's informed consent.

A **Trojan horse** is a program which seems to be doing one thing, but is actually doing another. A trojan horse can be used to set up a back door in a computer system such that the intruder can gain access later.

A computer **virus** is a computer program that can copy itself and infect a computer without the permission or knowledge of the owner.

A **vulnerability scanner** is a tool used to quickly check computers on a network for known weaknesses.

A computer **worm** is a self-replicating computer program. It uses a network to send copies of itself to other nodes (computers on the network) and it may do so without any user intervention. Unlike a virus, it does not need to attach itself to an existing program. Worms almost always cause at least some harm to the network, if only by consuming bandwidth, whereas viruses almost always corrupt or devour files on a targeted computer.

Attachment 3
Example of Major Security Incident, as reported in the May 8, 2009 edition of The Chronicle of Higher Education[7]

Hackers Access Medical Information of 160,000 in U. of California at Berkeley Database

San Francisco — Over a six-month period, a group of computer hackers accessed a database containing the medical information of more than 160,000 people associated with the University of California at Berkeley, including social security numbers and immunization records, Berkeley announced today.

Hackers gained access in October 2008 to the electronic medical records of Berkeley students, alumni, and their parents dating back to 2001. The compromised information includes social security numbers, doctor histories, and immunization records, but not specific diagnoses or treatments, the university said in a statement.

The breach lasted until April 9, when campus computer administrators noticed messages left behind by the hackers, according to the statement. The university immediately notified law enforcement authorities and today it began notifying students, staff, and others — including 3,400 students at neighboring Mills College whose information was also compromised because they were eligible to receive health care at Berkeley.

Security breaches involving social security numbers are not uncommon at colleges, but the length of time that hackers had access to university records is unusual, and university officials are certain to face questions about why they did not learn of the breach sooner. In addition to general medical information, hackers may have stolen the self-reported medical histories of students who studied abroad, the university said in an e-mail message sent to students, alumni and others.

"The university deeply regrets exposing our students and the Mills community to potential identity theft," Shelton Waggener, Berkeley's associate vice chancellor for information technology and its chief information officer, said in a statement. "The campus takes our responsibility as data stewards very seriously. We are working closely with law enforcement and information security experts to identify the specific causes that may have contributed to this breach and to implement recommendations that will reduce our exposure to future attacks." — *Josh Keller*

[7] http://chronicle.com/wiredcampus/article/3761/hackers-access-medical-information-of-160000-in-uc-berkeley-database