Information Security at ASU

Tina Thorstenson
Chief Information Security Officer
University Technology Office
infosec@asu.edu
data breach statistics

- 81% resulted from hacking
- 69% incorporated malware
- 10% involved physical attacks
- 7% employed social tactics
- 5% resulted from privilege misuse

Figure 17. Threat action categories over time by percent of breaches and percent of records

2012 Data Breach Investigations Report
securing our community

One University in Many Places

Confidentiality

Availability

Integrity
data breaches

Why University Security Matters

- Legal Obligation
  - FERPA
  - Graham-Leach-Bliley
  - Payment Card Industry Standards
  - AZ Breach Notification Statutes
- Reputational
- Moral Obligation

The Privacy Rights Clearinghouse tracks thousands of breaches involving millions of individual records
Thousands of new users come on our network each year, with thousands more departing.
We support nearly every kind of device on the consumer market.
Our large population of younger people more likely to take risks online.
Our IT organizations are largely decentralized which makes it difficult to deploy standard technologies or adopt standard policies.

ASU’s online user population exceeds 300,000 people.
ASU Information Security Program

- Overarching Policies & Standards
- Detailed Procedures & Guidelines
- Contractual & Regulatory Compliance
- Security Frameworks

- Preventative/Proactive Services
- Incident Response
- Security Reviews
- Risk Assessments
- Disaster Recovery/Business Continuity Planning

- Information Security Program
- Individual Security Projects
- Tools/Utilities Dissemination
- Defense In-Depth Strategies

- Formal Training Courses
- Outreach & Publication
- Website: getprotected.asu.edu
- Security Awareness for Students, Faculty, Staff & Affiliates
Here are a few of the current & recently completed initiatives:

- Secure border/network infrastructure
- Laptop encryption & mobile device security
- Securing web applications
- Secure personally identifiable information (PII)
effective practices

• keep it under wraps: don’t share your password

• length is strength: guess proof your passwords

• update often: stay safe with anti-virus, anti-spyware & anti-malware

• don’t get hooked like a phish: beware of anonymous emails
effective practices

- be careful where you surf: some websites are harmful

- if you don’t need it, delete it: trash unnecessary data

- protect with pins, passwords and 2-factor: use pins and passwords to secure your computer, phone & other mobile devices

- encryption is key: encrypt your computer, flash drive, phone & other mobile devices to prevent others from stealing your data
tips & tricks for department systems & servers

• Review systems and accounts for unnecessary access.

• Review server and system logs regularly. Set system automated alerts for unusual activity.

• Perform security scans on all of your web applications.

• Set your browser to block pop-ups, flash movies, scripts, etc. Most tools will let you whitelist the good stuff with a click or two.

• Keep systems patched; apply vendor security maintenance promptly.
report security events

- To report an event or incident, contact the ASU Help Desk at 1-855-278-5080.

- For events that do not require an immediate response, email the Information Security Team directly at infosec@asu.edu or visit getprotected.asu.edu.
Questions?

Tina Thorstenson
Chief Information Security Officer
University Technology Office
infosec@asu.edu