ANNUAL SECURITY RESPONSIBILITY REVIEW

For Faculty and Staff Who Use Computers Minimally in their work

May 2012

CAL POLY
SAN LUIS OBISPO
INFORMATION SERVICES | OFFICE OF THE CIO

Training Topics

- What is Information Security?
- Review Security Vulnerabilities
  - Phishing email messages designed to trick you into providing confidential information
  - Not securing your password
  - Handling confidential information
- Your Security Responsibilities
- Who to Contact for Help

What is Information Security?

- Information security is the protection of university information in all of its forms (printed, electronic, spoken)

- Everyone has a responsibility to prevent unauthorized access, disclosure and misuse of university information, and to report suspected abuses

What is Phishing?

- Phishing is a tool used by cyber criminals to steal personal information from another person using an email message which:
  - appears to be from a trusted source - your employer, bank, or online account
  - asks you to enter confidential information (passwords, account numbers, SSN, etc.)
  - may provide a link to a fake website
- Criminals will then use the information provided to buy stuff, and transfer money out of your account.

Phishing Email Messages

Protect Yourself From Phishing Email

- When you receive an email requesting personal information, ask yourself:
  - Who is asking?
  - Why would they ask for this?
  - Why would they need it?
  - Could this information lead to identity theft, credit card fraud, loss of money, or allow others to gain unauthorized access to Cal Poly protected information?
- Don't reply to emails asking for confidential or personal information.
- Don't click on embedded links in emails asking for confidential information.
- Follow your "gut feeling" and don't respond to suspicious email messages.
- A legit company won't ask for this

Time for a Password Change?

CAL POLY
SAN LUIS OBISPO
INFORMATION SERVICES | OFFICE OF THE CIO

Password Tips

- Use a strong password that is hard to guess
- Avoid using the same password for multiple accounts
- The password used for Cal Poly access should not be used anywhere else
- Passwords are confidential - Don’t share them!
- Logged out and close your browser when finished
- Lock your workstation when away from your desk

Protecting Passwords

- **No one should ever ask you for your account or password**
  - No Cal Poly, CSU, or reputable company should ever ask you for this information
- **If you're ever asked (in an email or over the phone), do not give it out!**
- **If you suspect your Cal Poly password has been compromised:**
  - Contact the ITS Service Desk (805-756-7000) and change your password immediately!
  - Report the incident to abuse@calpoly.edu

Handling Confidential Information

The CSU defines protected information as Level 1 and Level 2

- Level 1 data is protected by a variety of laws and regulations (includes personally identifiable information - SSN, passwords, credit card information, birthdate, driver's license number, etc.)
  - Risk Level – High

- Level 2 data must be protected due to ethical, privacy and proprietary considerations (includes EmplID, student education records and employee information - home address/phone, etc.)
  - Risk Level – For Internal Use Only

- Level 3 data is public information
  - Risk Level – Publicly Available

Uh-Oh!

I may have Level 1 or Level 2 data.

What should I do?

Learn By Doing

- If you find protected data in a public place or simply discarded in a trash can or recycling bin, move it to a secure location and report it as soon as possible to your supervisor
- Protect physical spaces against unauthorized access or use (lock doors, monitor traffic, etc.)
- Never use someone else's computer to surf the web or send emails; only use resources that you are authorized to use
- When speaking about a confidential matter, make sure your conversation cannot be overheard by unauthorized persons
- Never use a jump drive or other electronic device you happen to find somewhere; such devices may contain protected data or malicious software; report it to your supervisor

Security Responsibilities - 1

- Responsible Use Policy
- Applies to anyone who uses Cal Poly's IT resources
  - All users are expected to be familiar with and abide by this policy
  - With each portal password change, you must agree to abide by the campus responsible use policy and indicate you have read it:
  - To review the policy, go to: http://security.calpoly.edu/policies/rup/
- All Cal Poly users are responsible for:
  - ensuring the confidentiality and appropriate use of Cal Poly data to which they are given access,
  - ensuring the security of the equipment where such information is held or displayed, e.g., making sure offices and workstations are locked,
  - ensuring the security of any accounts/passwords issued in their name, and
  - abiding by related privacy rights of students, faculty, and staff concerning the use and release of personal information

Security Responsibilities - 2

- As an employee at Cal Poly you have access to information which must not be shared
  - This may include personnel, financial, and student records.
- Everyone affiliated with Cal Poly who has access to university information and resources are required to sign a confidentiality-security agreement form acknowledging responsibility for data protection
- Use your good judgment: if you're not sure of what is acceptable or allowable or not, please ask your supervisor or manager for assistance
- Learn more about information security and safe computing practices at http://security.calpoly.edu

Who to Contact for Help

- Seeking Advice & Reporting Violations
  - Unclear on if, when and how this applies to you?
  - Unsure about what to do in a given situation?
  - Believe a potential vulnerability may exist?
  - Suspect a potential violation has occurred?
- Notify
  - Your manager, supervisor or department head
  - Cal Poly's Information Security Office
  - abuse@calpoly.edu