Berkeley
UNIVERSITY OF CALIFORNIA

Micronet Meeting
April 27, 2011

Security, Privacy, and Policy

Ann Geyer
Karen Eft
Matt Wolf

SPP Charter

- Protect individual privacy
- Reduce campus risk
- Safeguard information and IT assets
- Inform campus leadership
- Educate data owners and users

Protect Individual Privacy

- Advance a culture of privacy
- Oversee ECP compliance
- Reduce the collection & retention of private information
- Promote the separation of identity from data

Reduce Campus Risk

- Conduct risk assessments
  - 3 Tiered Approach—Self, Facilitated, DSR
- Classify & treat data on the basis of risk
  - Notice Triggering Data is designated High Risk
  - SSN, Credit Cards, Medical, Financial
- Promote better security practices
  - MSS-EI
  - Management Oversight

Safeguard Information & IT Assets

- Minimum Security Standards
- Security Best Practices
- Recommended security protections by data risk categories
- Policy and standards compliance
- More informed risk decisions

Inform & Educate

- Campus Leadership
  - Risks and Metrics
- Data Owners
  - Roles and Responsibilities
  - Methods and Tools
- Users
  - Cyber Self-Help
  - Basic Security & Privacy Protections

SPP Team

Direct Reports

- Erika Donald
  - Education & Awareness
  - Security Administration
- Karen Eft
  - Policy Management
  - ECP Oversight
- Matt Wolf
  - DSR program

Close Relationships

- Privacy Officers
  - UHS
  - Opt Clinic
  - Psych Clinic
  - Registrar (Students)
  - CPHS (Research)
- Security Officers
  - Student Services
  - UHS

ISC² Security Domains	Roles
Security Management (Oversight, security roles & responsibilities, risk management, data classification, documentation, metrics, awareness)	SPP
Access control systems and methodology (identification, authentication, authorization, accounting)	Data owners Identity Mgt
Security architecture and models (access control, integrity, data flow)	Security & Privacy Officers IT
Cryptography	
Business continuity and recovery planning	Bus Resumption Group
Application and systems development security (conception, development, implementation, testing, and maintenance)	Developers PMO
Telecommunications and networking security	SNS
Operations security (hardware & software controls; auditing & monitoring)	Desktop support SNS
Physical security	UCPD
Laws, investigation, and ethics	Legal, Audit, Compliance

Berkeley
UNIVERSITY OF CALIFORNIA

Policy Management

Karen Eft

Policy manager

- Policy and standards compliance

- Reduce campus risk
  - Policy reviews, updates
  - Procedures
  - Consultation

Important activity areas:

- They reflect upon UCB
  - Berkeley.EDU domain name
    - *Email, blogging, hosting*
  - copyright infringement allegations
    - *DMCA, subpoenas, HEOA*
- They require access to electronic information
  - to continue departmental business
  - as evidence for investigations

Access procedures

ECP = “electronic communications” policy

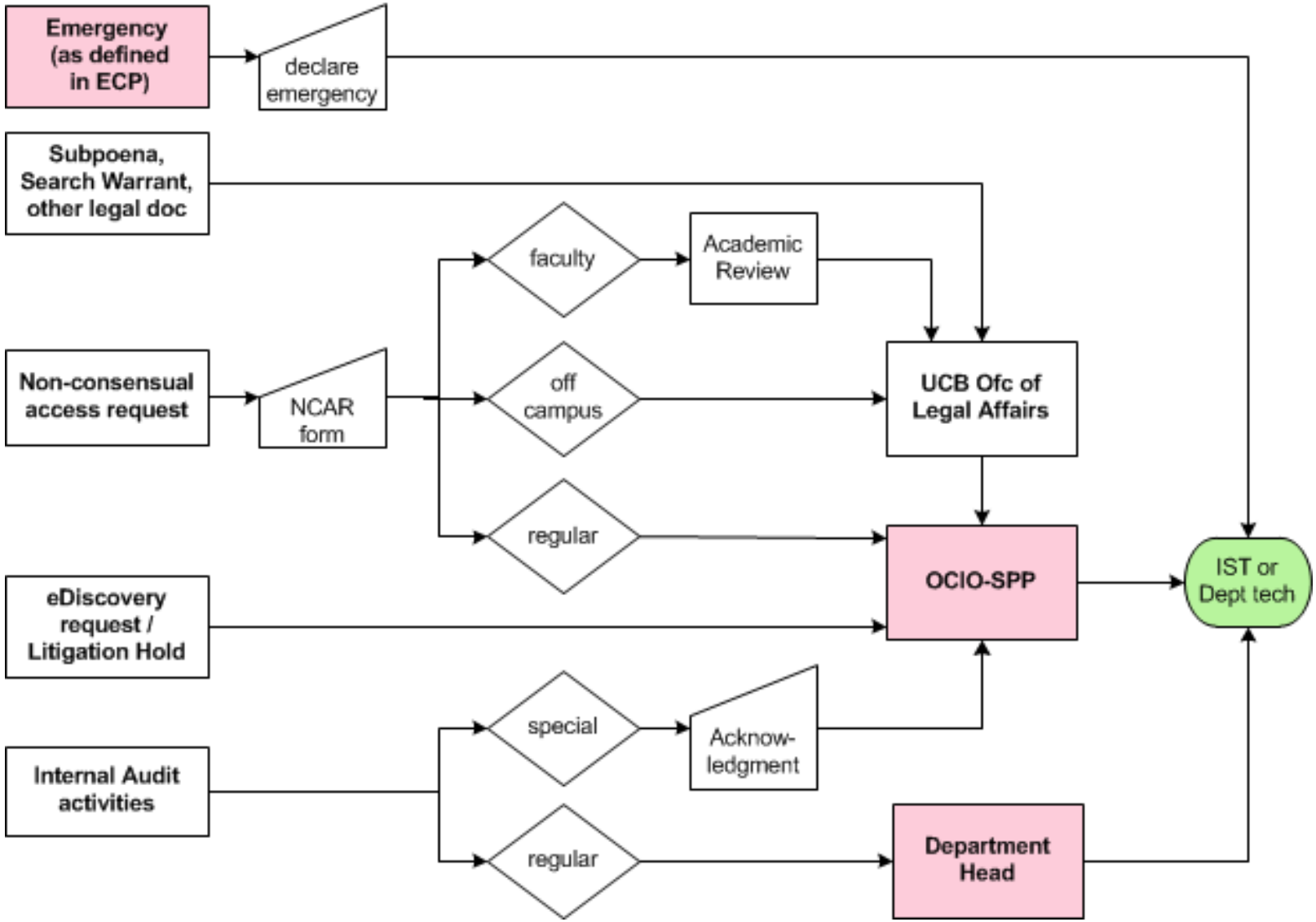
1. asked by employee to help with their email technical problem -- you “have the holder’s consent” to access it
2. for continuity of departmental business

   use dept’l email account or shared space

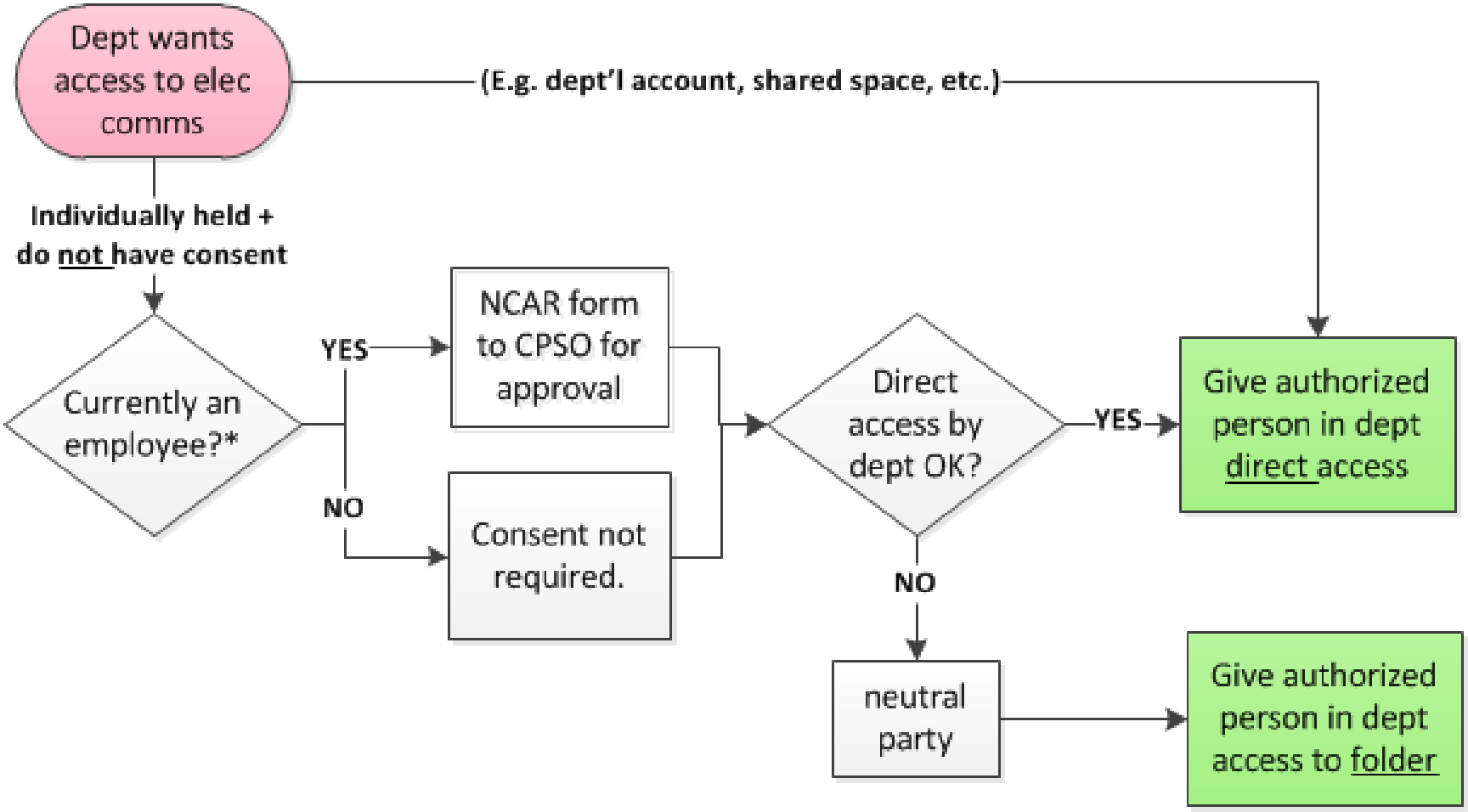
-- or --

3. must follow non-consensual access procedures

Access w/o consent



Coordination with tech support



Responding to Requests for Electronic Evidence

See the Key to abbreviations, below.	Federal or State law		University or Campus Policy	
	Preserve?	Divulge?	Preserve?	Divulge?
Civil law – when a court case has been filed	E, P	S	—	—
Civil law – legal action "reasonably anticipated"	E, P	M	—	—
Criminal law – when a court case has been filed	P	S	—	—
Criminal law – legal action "reasonably anticipated"	M	M	—	—
Federal agency or other law enforcement agency request for electronic information (including police):				
a. information does not reveal activities of UCB individuals	M	M	—	—
b. information **does** reveal activities of UCB individuals:				
• **Without** Preservation Order or other appropriate written authorization	X	X	—	—
• **With** written auth (and UC Counsel legal review)	P	S	—	—
Internal Audit investigating	P	D	P	D
Misconduct – Campus OHR investigating	—	—	P	A or S
Misconduct – Student Judicial Affairs investigating	—	—	P	A or S
Misconduct – others investigating	—	—	P	A or S

… Electronic Evidence (cont'd)

Key:

A = Access allowed if you have written consent of the holder* —or— follow UC Electronic Communications Policy (ECP) procedures for approval of access without consent.

D = Divulge as requested.

E = Preservation is required within the bounds of "e-Discovery" rules, with few exceptions. See New Federal "e-Discovery" rules affect IT practices (Spring 2007 iNews).

M = Maybe; i.e. depends who's asking. Need more information to determine.

P = Preserve if not too burdensome (requires discussion to clarify).

S = Subpoena, warrant, NSL, Preservation Notice, etc. upon UC/UCB legal counsel-approval of written legal instrument (e.g. to determine whether the activities involved in preservation would inappropriately compromise required secrecy, along with their review of other legal issues).

X = Do not preserve/divulge.

* Systems administrators and other operators of University electronic communications services are excluded with regard to electronic communications not specifically created by or addressed to them.

http://technology.berkeley.edu/policy/evidence.html

Guidelines for administering appropriate use (for service providers)

A. Defining Appropriate Use

B. Ensuring Compliance

C. Termination of Accounts

D. Responding to Allegations of Misuse

E. Access Warning Statements

APPENDIX

A. RESOURCE OFFICES

B. SELECTED REGULATIONS AND PROCEDURES

C. DOCUMENT EXAMPLES

D. EDUCATIONAL OPPORTUNITIES

https://technology.berkeley.edu/policy/approp.use.html

Berkeley
UNIVERSITY OF CALIFORNIA

Data Security Review Program

Matt Wolf

Table of Contents

Overview - Data Security Reviews

- The Basics
  - Risk – Data Theft
  - Threats – Network-Based and Physical
  - Process – Discovery, Classification, Assessment and Reporting/Guidance

- Units Reviewed in 2010
  - Financial Aid (ProSAM)
  - University Extension
  - Residential and Student Service Programs - Cal1Card
  - Audit and Advisory Services
  - University Relations

Risk of Data Theft to UC Berkeley

- Financial
  - Cost for breach notification and associated investigations
- Regulatory / Compliance
  - HIPAA
  - PCI
  - FERPA
  - Federal Trade Commission Act
- Litigation
  - Class-action lawsuits
- Reputational
  - Alumni development
  - Business relationships

Finding: No Data Inventories

- Summary of Risk
  - Effective management of security requires accurate inventory
  - Without inventories, incorrect or ineffective controls may be applied
- Supporting Data
  - No written inventories of notice-triggering data stored electronically or on paper
  - In 4 out of 5 units, notice-triggering data found in unknown and unexpected locations

Finding: Unpatched Software Vulnerabilities

- Summary of Risk
  - Vulnerabilities in software may be exploited to compromise systems resulting in data theft

- Supporting Data
  - No effective strategy for patching software in 4 out of 5 units
  - More than 2,500 campus machines compromised per year – 80% as a result of inadequate patching
  - Number of vulnerabilities in third-party software increased by 71% in 2010

Finding: Insecure Application Development

- Summary of Risk
  - Insecure code may be exploited by attackers to compromise systems and steal data.

- Supporting Data
  - Of the units who develop software, all fail to:
    - Train developers on secure coding practices
    - Code applications securely
    - Separate development and production environments and data
    - Review application security vulnerabilities
  - Root cause of two recent breaches

Finding: Insufficient Logging and Monitoring

- Summary of Risk
  - Complicates forensic analysis of security events
  - Compromises remain undetected

- Supporting Data
  - 4 out of 5 units did not effectively collect logs
  - None effectively monitored logs
  - Serious compromises undetected for months

Finding: Weak Department Level Security Controls

- Summary of Risk
  - Poor controls result in insufficient defense-in-depth and increase the likelihood of data theft.

- Supporting Data
  - Overly permissive or missing firewalls in 4 of the 5 units
  - No hardening to an industry-recognized security standard
  - Inappropriate use of shared credentials
  - Access control lists for file and database servers allowed more access than necessary

Berkeley
UNIVERSITY OF CALIFORNIA

Education & Awareness

Erika Donald

Processes and Publicity

- Erika Donald
  - Education & Awareness
  - Security Administration

itpolicy@berkeley.edu

abuse@berkeley.edu

security-policy@berkeley.edu

Current Security Initiatives

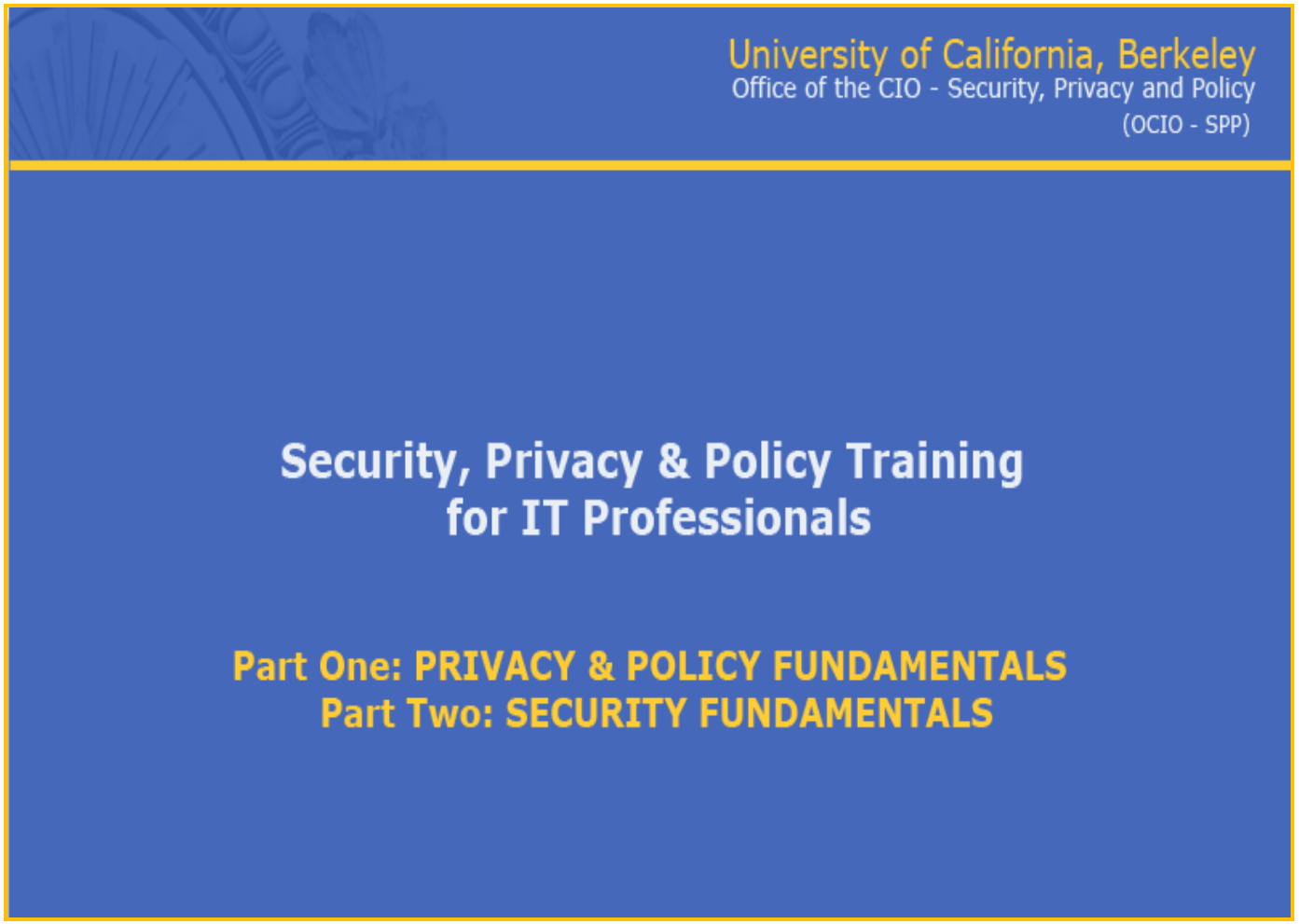
- Approval to use SSNs
- Copyright infringement allegations
- Offsite use of campus domain name
- Exception Requests for Minimum Security Standards

How do I …

- Report threats of physical harm?
- Get exceptional approval to examine or disclose electronic communications records?
- Request early disabling of CalNet or CalMail accounts?
- Respond to online copyright infringement allegations?
- Get help with security breaches / data breaches?
- Handle electronic evidence?
- Respond to objectionable electronic communications?
- Request an exception to computer security requirements?
- Request off-site hosting?
- Get help with information technology policy issues?

http://technology.berkeley.edu/policy/How-do-I.html

Education


University of California, Berkeley
Office of the CIO - Security, Privacy and Policy
(OCIO - SPP)
Security, Privacy & Policy Training
for IT Professionals
Part One: PRIVACY & POLICY FUNDAMENTALS
Part Two: SECURITY FUNDAMENTALS

Awareness

Now

- posters
- pamphlets
- charts
- photos

Future

- video clips
- “you tell us”

Don’t take the bait!

If you receive “phishy” emails like these:

Dear CalMail User,

To keep your account from closing, you must update:

Name:
Username:
Password:
Date of Birth:

Congratulations!

You’ve won a FREE $500 Mervyn’s gift card!

Participation required. Click here for details.

Someone wants your personal information.

Official services will never ask for your password!

- **Never respond**
  Don’t ever send your personal information or password—even if it looks like the email comes from UC Berkeley, the FBI, your bank, PayPal, etc.
  Also, don’t click on links in unsolicited emails!
- **Don’t be fooled**
  Phishing emails can look genuine because your name and other personal information can be obtained from social media sites.
- **Report it**
  Forward suspicious email sent to your campus account to consult@berkeley.edu.
  If your computer has been compromised as a result of phishing, contact your local IT support staff or send email to security@berkeley.edu.

UC Berkeley Office of the CIO Security, Privacy & Policy

Summer 2010

Awareness:

- Use of Social Media
  - For Students and Staff
  - For Departments and the University
- Before sourcing your technology…
- Protect Your Privacy
- Privacy Resources and Contacts