Data is Forever - Don't Give it Away

Julianne Tolson
Information Security Officer

Information Technology Services

SF STATE

Data is Forever - Don't Give it Away

- What information do you share?
- Data generated and stored throughout your life
- What you can do to protect your data
- Weakest link identity hack scenarios
- What you can do to protect others
- Q & A

What are your information “secrets”?

- ❑ Diagnoses / Height / Weight
- ❑ What you buy / Net Worth / Debt
- ❑ Grades / Performance evaluations
- ❑ Disciplinary actions / Arrest record
- ❑ Experiences / Relationships / Feelings
- ❑ Web search queries & sites visited
- ❑ Other _____

What information do you consider public?

- ❑ Name
- ❑ Employer
- ❑ Work address
- ❑ Work phone
- ❑ Work email
- ❑ Education
- ❑ Degrees & Certifications
- ❑ LinkedIn profile
- ❑ Gross salary

What information do you provide when requested?

- ❑ Age / Birthday
- ❑ Personal Email
- ❑ Home Phone / Address
- ❑ Income bracket
- ❑ Relationships / Family
- ❑ Associations / Interests
- ❑ Hometown
- ❑ Volunteer activities
- ❑ Religious beliefs
- ❑ Political beliefs

What information do you provide when required?

- ❑ Expenses
- ❑ Income
- ❑ Net Worth
- ❑ Credit/debit card
- ❑ Bank account
- ❑ Social Security Number
- ❑ Drivers License
- ❑ Passport

Think about personal data generated and stored throughout your life – part 1

- ❑ Medical
- ❑ Birth certificate
- ❑ Social Security
- ❑ Passport & Immigration
- ❑ Education
- ❑ Organizations – scouts, sports, affinity, religious
- ❑ Bank

Think about personal data generated and stored throughout your life – part 2

- ❑ Driving
- ❑ Insurance
- ❑ Employment
- ❑ Law enforcement
- ❑ Voter
- ❑ Certifications
- ❑ Housing
- ❑ Utilities
- ❑ Retail

Think about personal data generated and stored throughout your life – part 3

- ❑ Juror
- ❑ Taxes
- ❑ Credit / Loan
- ❑ Census
- ❑ Relationship – marriage, domestic partnership, children
- ❑ Property
- ❑ Court records
- ❑ Death

Where is your information stored?

- ❑ Paper
- ❑ Fiche/film
- ❑ Tape
- ❑ CD/DVD
- ❑ USB Drive
- ❑ External hard drive
- ❑ Internet accessible storage

Think about the organizations you are no longer in contact with

- ❑ Schools
- ❑ Tax preparers
- ❑ Medical providers
- ❑ Financial institutions
- ❑ Businesses
- ❑ Employers
- ❑ Social organizations
- ❑ Online friendship services
- ❑ Former landlords

Where is that data now?

- ❑ Stored securely
- ❑ Destroyed securely
- ❑ Stored in a non-secure manner
- ❑ Disposed of in a non-secure manner
- ❑ Sold
- ❑ Lost
- ❑ Unknown

What you can do to protect your data

Ask why before providing any personal data

- ❑ Leave blank where no benefit
- ❑ Walk away – call or go in person
- ❑ Consider providing “alternative facts” where no consequence
- ❑ Guard your identity unique identifiers - primary keys (SSN, DL, Passport)

What you can do to protect your data

Manage your passwords

- ❑ Use a password management system
- ❑ Carefully select password reset questions and answers
- ❑ Use two-factor authentication for high risk accounts

What you can do to protect your data

Keep accounts separate and discrete

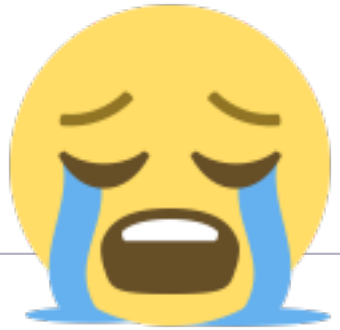
- ❑ Consider same username repercussions
- ❑ Don’t mix business and pleasure
- ❑ Don’t use the same password for different sites
- ❑ Review your weakest links

Weakest link scenario 1

Compromised Facebook password

- ✓ Instant access to: education, interests, relatives, friends, activities, birthdate, phone, email, work, religion, photos, messages, ip addresses, hometown, credit card –facebook history including searches
- ✓ Access any other account using same password, username or email to login

Weakest link scenario 2



Compromised personal Email account password

- ✓ Review email to determine which accounts to try
- ✓ Use to reset and access all accounts that were registered with that password
- ✓ Use SF State password reset to send reset code to personal email account
- ✓ Access university records

Weakest link scenario 3

Enter a contest

1. contest is a scam OR
2. contest is legitimate but data stored in plain text and accessed by hackers

✓ Provided name, email address and selected password used for other accounts

✓ Access any other account using same password, username or email to login

What you can do to protect others

Ask why before requesting personal data

- Less is more – can you link to related data
- Use SF State ID or email as identifier
- Have a documented business reason for collecting and storing confidential data
- Guard identity primary keys (SSN, DL, Passport)

Confidential data is a high risk activity

1. Conduct risk assessment of storing data
2. Identify and document custodian of records
3. Inventory and track data through all stages
4. Collect as little data as possible
5. Transfer data securely using encryption
6. Store data securely using encryption
7. Process data using access controls – authentication and authorization
8. Evaluate retention schedules and business need to retain data
9. Destroy data in a secure manner

SF STATE