Privacy Awareness Training
Protection of Personal Information

Ron Woerner

NEbraskaCERT Conference 2006

Why am I here?

What's in it for you?

What is privacy?

Why is maintaining data privacy important to your organization?

What can I do to protect data privacy?

Today's Training Agenda

Why we need to protect privacy

Privacy Laws, Regulations & Standards

California Law – SB1386

Introduction to HIPAA

What you should do

Q&A

What is Privacy?

"The right to be let alone" - *Supreme Court Justice Brandeis, 1890*

The right of individuals to control the collection and use of personal information about themselves. – *Privacy Journal*

The Problem

Constantly advancing technology permits:

- The collection and aggregation of large quantities of data,
- In any desired format or structure,
- Subject to endless permutations of sorting, filtering and analysis, and
- The instantaneous widespread distribution of the raw data or analysis results

… all without significant human thought.

Increasing the Risk of a Privacy Meltdown

Information technology – accumulate, link and share massive amounts of personal information;

Data perseverance – personal information may be stored anywhere, often without any protections;

Data classification – personal information may not be classified.

Interconnectivity of businesses – information shared among affiliates and associates;

Web-based delivery of products and services facilitate collection and tracking; disclosures have bigger impact – on a much larger scale.

The Problem


IT IS HARD WALKIN' ON THIS STUFF.
YEP, SON, WE HAVE MET THE ENEMY AND HE IS US.
CYBERSPACE

THIS HAS HAPPENED AND CONTINUES TO HAPPEN!

THIS HAS HAPPENED AND CONTINUES TO HAPPEN!

–November 2004: *ChoicePoint* — Identity theft involving 145,000 persons
–December 2004: *Bank of America* — 1.2 million records misplaced
–January 2005: *T-Mobile* — Illegal access to 16.3 million records
–January 2005: *HSBC* — 180,000 MasterCard records stolen
–February 2005: *Ameritrade* — 200,000 customer files lost
–March 2005: *LexisNexis* — Identity theft involving 32,000 records
–March 2005: *DSW Inc* — Hacker theft of 103 credit card numbers
–March 2005: *Boston College* — Theft of 120,000 alumni donor records
–April 2005: *TimeWarner* — Lost files on 600,000 employees
–June 2005: *Citibank* — Backup tape containing personal information on almost 4 million customers was lost by UPS delivery service
–Last Month: *Union Pacific* – Lost laptop with 30,000 employee records
–Last Week: *Veterans Administration* – Stolen laptop with 26 million records

Identity Theft – constant problem

Identity Theft

CITI – Identity Theft Commercials

http://www.fightidentitytheft.com/citibank-idtheft-commercials.htr

What it is?

When someone uses the identifying information of another person such as name, social security number, mother's maiden name or other personal information to commit fraud or engage in other unlawful activities.

Since October 1998, identity theft is a crime.

Scary Statistics

- In 2003
  - 251,000 Identity Theft (IDT) Victims – up from 162,000 in 2002
  - 781 IDT Victims from Nebraska (Omaha - 374)
  - 28% of IDT Victims were in their 20s
  - 42% of FTC complaints were IDT, up from 40%
  - 55% of fraud cases were internet, up from 45%
- It costs up to $2,000 for the victim to clear his/her name.

Identity Theft Methods

- Internet
  - Phishing
  - Spyware, adware, tracking cookies, etc.
- Lost or stolen wallets and purses
- Mail theft
- Fraudulent change of address
- Dumpster diving
- Inside sources

Identity Theft Methods

- Internet
- Lost or stolen wallets and purses
- Mail theft
- Fraudulent change of address
- Dumpster diving
- Inside sources
- Social Engineering

What's in your wallet ?

Open your wallet, and look what's inside:

- SSN
  - Card
  - Insurance Cards
- Credit Cards
- Driver's License
- Pre-paid cards
  - Phone
  - Restaurant
- Signed checks
- Phone contacts
- Store or Bank Receipts

What happens

- Open a new credit card or bank account in the victim's name using stolen information.
- Change the address on credit or bank accounts.
  - This delays problem identification.
- Charge items under the victim's name.

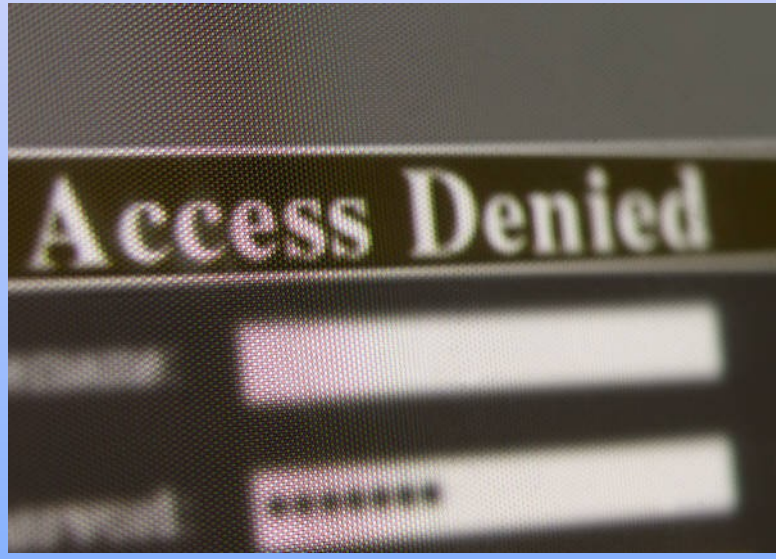
  May include:
  - High price items
  - New services (phone, wireless, etc.)
  - Auto loans

What You Can Do

Identity theft cannot be stopped completely.

Risk reduction activities

- Internet fraud
- Personal protection



Trust, but Verify

Minimizing Risk – Internet Fraud

- Don’t reply to emails or pop-up messages asking for personal or financial information.
- Go directly to the web site instead of following links in emails requesting you update personal information.
- Be selective of the web sites you visit, but more importantly, be cautious of the content you click on.
- Don’t open attachments or download files from strangers.
- Automatically update anti-virus software.
- Don’t forget to contact the FTC about suspicious activity (e.g., spam@uce.gov)

Minimizing Risk – Personal Protection

- Carry the minimum number of credit cards in your wallet or purse. Do not carry your social security card.
- Don’t use personally identifiable information when selecting a pin or password.
- Keep items with personal information in a safe place (even at home).
- Make sure you get and scrutinize monthly statements.
- Opt-out when possible.

Minimizing Risk – Personal Protection

- Invest and use a personal cross-cut shredder.
- Be careful leaving outgoing checks or paid bills in your residential mailbox.
- Order a copy of your credit report at least once per year.
- Don’t give out personal information over the phone unless you initiated the call.
- Don’t give out personal information (esp. SSN) if you don’t have to.

Use of Social Security Number (SSN)

If someone other than your employer, financial institution or loan officer requests your SSN, ask:

- Why do you need my SSN?
- How will you use my SSN?
- What law requires me to give you my SSN?
- What will happen if I don't give you my SSN?
- Can I use a different number instead?

Don't be intimidated into giving your SSN.

The decision is yours.

If You're a Victim

1. Get the FTC ID Theft document

   http://www.ftc.gov/bcp/conline/pubs/credit/idtheft.htm

   1. Read it
   2. Use the forms in it

3. Contact the fraud departments of each of the three major credit bureaus.

   1. Tell them you're and identity theft victim.
   2. Request a "fraud alert" be placed in your file.
   3. Order copies of your credit report.

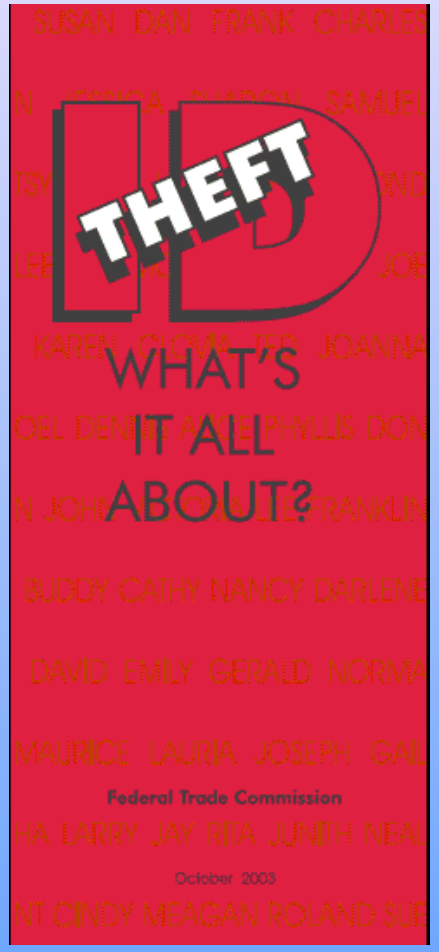
If You're a Victim

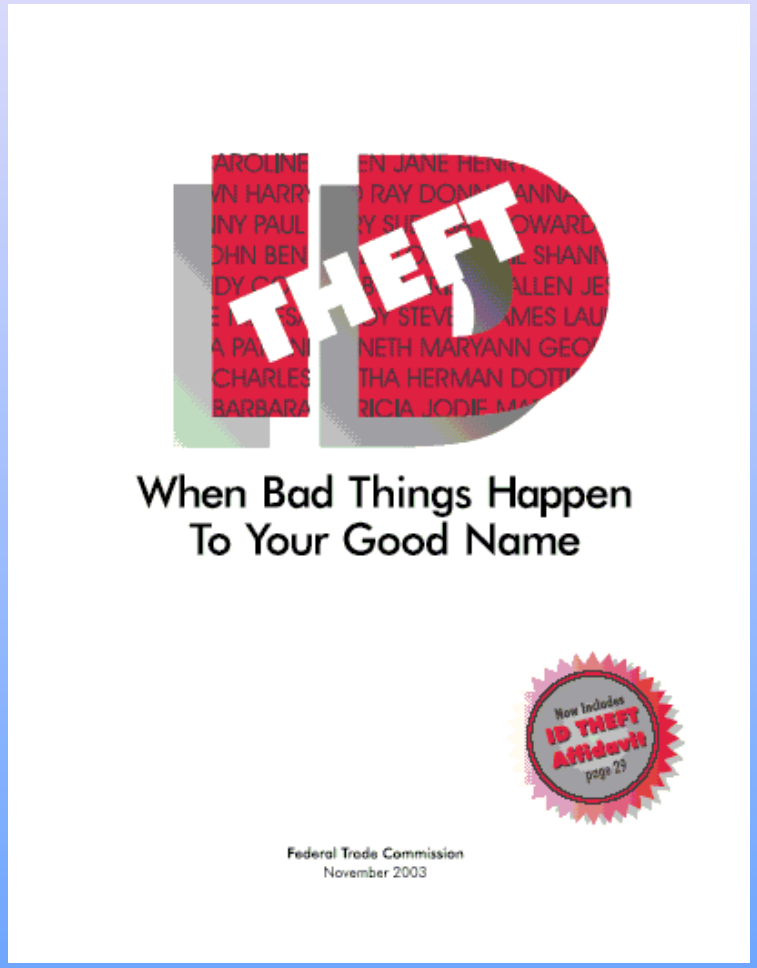
1. Close accounts you know or believe have been tampered with or opened fraudulently.
    1. Bank accounts
    2. Credit cards
    3. Phone & Utilities
2. Complete the FTC ID Theft Affidavit or company's fraud dispute form.

    http://www.consumer.gov/idtheft/affidavit.htm
3. File a police report.

FTC Resources

http://www.consumer.gov/idtheft/





What is Personal Information?

Personal Information includes “an individual's first name or first initial and last name in combination with one or more of the following”*:

- a social security number,
- drivers license number or other identification card number,
- account number, and/or credit or debit card information including numbers and passwords, PINs and access codes.

Personally Identifiable Information (PII) may also include:

- Address
- Phone number

* From California Law SB1386

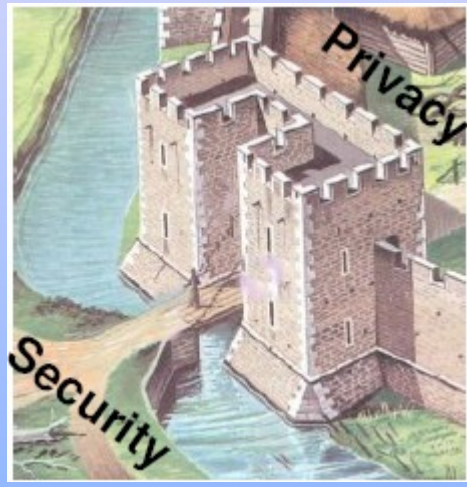
More Definitions

Data Privacy – The evolving relationship between technology and the legal right to, or public expectation of privacy in the collection, storage and sharing of personal data.

HIPAA Privacy – Rules that safeguard the privacy of individually identifiable health information by placing limits on its use and disclosure.

Electronic Data Interchange ("EDI") – Rules that standardize transactions and code sets for the electronic data interchange of health information.

Information Security – Rules that protect the confidentiality and integrity of data in electronic media, including the prevention of unauthorized use and restriction of physical access to such data.



Where does Your Organization collect, store, process and disclose private data?

- PeopleSoft
  - Oracle databases
  - PeopleFinder
- E-Mail & Attachments
- Workstations
- Storage / Shared drives
- Servers
  - Web servers
  - Ecommerce servers
- Other Applications

How can you come into contact with personal or private data?

The Problem

How do we determine and implement adequate and appropriate protection for personal information collected, stored or processed at ConAgra Foods?

Protecting Privacy Is Everyone's Responsibility

Universal Participation

A privacy program must involve all personnel, computer systems, and implementation logic.

It's up to you to help protect data.

It is not just "The Company". Each one of us can be held liable and accountable.

- Financially
- Occupationally
- Criminally

Handling Sensitive, Personal Data

Methods for handling sensitive data:

- Data Classification
- Encryption
- Access Controls
- Segregation of Duties
- Help Desk
- Disposal Procedures

Follow the current standards and controls.

Handling Sensitive, Personal Data

What you should do if you encounter personal data:

- Open a Help Desk ticket
- Contact your manager and Information Security
- Take steps to secure it

Benefits of Strong Privacy Policies and Practices

- Strong organizational image and competitive edge
- Potential for expansion into jurisdictions requiring adherence to strong standards
- Enhanced data quality and integrity fostering better customer services and strategic decision making
- Enhanced customer/consumer trust and loyalty
- Savings in terms of time and money
- Conforming with Privacy Legislation
- Better informed employees make better decisions

Consequences of Privacy Breaches

- Damage to an organization's reputation, brand image, and business relationships
- Psychological and economic harm to customers
- Loss of customer/consumer trust and loyalty
- Financial losses due to deterioration in data quality and integrity resulting from lack of trust
- Loss of market share and drop in stock prices following a privacy incident or cancellation or delays in roll out of new products and services due to privacy concerns
- Violations of privacy legislation

Negligence –T.J. Hooper Case

Setting the rule (1932):

Tug boat lost barge and coal during a storm. Barge owner claimed negligence because the Tug didn't have a weather radio.

Supreme Court found that there is a duty to keep up with technological innovations that set the standard of care in the industry. A breach of that duty of care is actionable negligence.

"there are precautions so imperative that even their universal disregard will not excuse their omission."

U.S. Privacy Laws

Fair Credit Reporting Act
Privacy Act of 1974
Family Educational Rights and Privacy Act
Right to Financial Privacy Act
Privacy Protection Act of 1980
Electronic Communications Privacy Act
Video Privacy Protection Act
Employee Polygraph Protection Act
Telephone Consumer Protection Act
Health Insurance Portability and Accountability Act
Driver's Privacy Protection Act
Identity Theft and Assumption Deterrence Act
Gramm-Leach-Bliley Act (Title V)
Children's Online Privacy Protection Act

Additional U.S. Privacy Laws

Computer Fraud and Abuse Act (criminalizes hacking and break-ins)

The Federal Trade Act (has general anti-fraud and safety authority)

Cable Communications Policy Act (protects subscribers from having their private information shared)

Telecommunications Act of 1996 (protects subscribers from unauthorized use of their personal information)

The Foreign Intelligence Surveillance Act of 1978 (permitting surveillance without a court order)

The Patriot Act (which alters many of the foregoing) Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001

Privacy Laws Affecting My Company

Federal Trade Commission

California Privacy Law SB 1386

Nebraska Privacy Law LB 876

U.S. Federal Laws

Health Insurance Portability and Accountability Act (HIPAA)

Children's Online Privacy Protection Act (COPPA)

Canadian & European Union Laws

- EU *Directive on Data Protection* led to expansion of privacy laws in many countries around the world
- U.S. Safe Harbor provisions addressing EU privacy directive
- Canadian *Personal Information Protection and Electronic Documents Act*

Federal Trade Commission

Speaking before a Senate panel investigating possible national legislation aimed at better data protection, FTC Chairman Deborah Majoris stated,

"For the first time we allege that inadequate data security can be an unfair business practice. This action should provide clear notice to the business community to establish and maintain reasonable affirmative security measures."

Speaking on the ChoicePoint data breaches, she said,

"The message to ChoicePoint and others should be clear: Consumers' private data must be protected from thieves."

*California Privacy Law SB 1386**

Disclosure of Personal Information

Notification

Data Encryption

Authorization

*32 States now have similar laws and many others are pending.

Nebraska Privacy Law LB 876

Effective July 13, 2006

Definition of Personal Information more broad than the California Law

Requires encryption and redaction or other methods to make data unreadable/unusable

Breach obligations similar to California except:

- Entities must undertake an investigation when a breach occurs;
- Notice is only required if unauthorized use of the compromised PI has occurred or is likely to occur.

Objectives of HIPAA

Health Insurance Portability and Accountability Act (HIPAA)

Primary goal – to assist in the portability of health insurance and to reduce the administrative cost of healthcare.

Establish accountability for Protected Health Information (PHI)

Prevent misuse of health information

Provide individuals with greater control over their health information

Establish safeguards for health information privacy and security

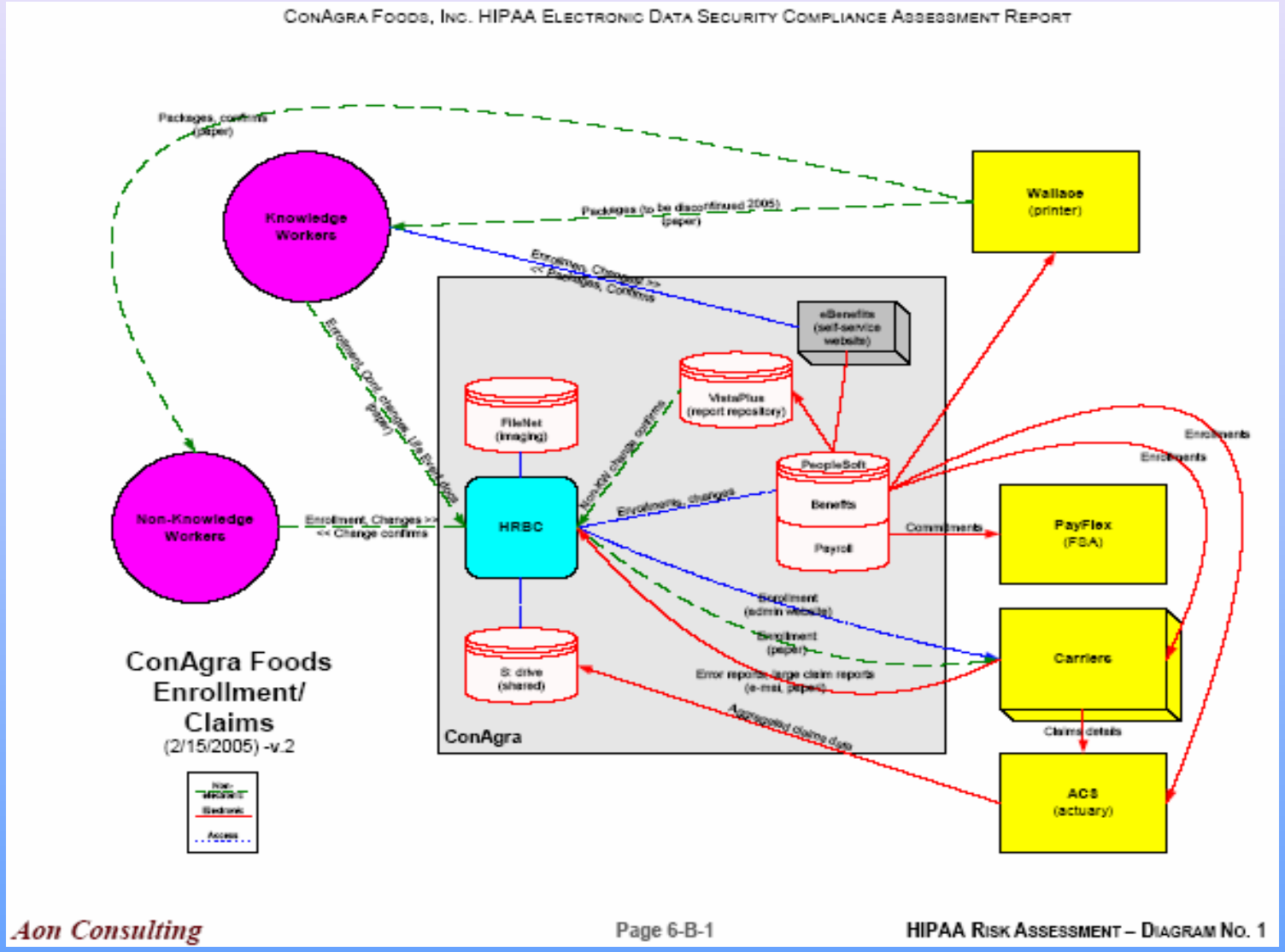
What Is Protected Health Information (PHI)?

Health Information that is:

- Created or received by a Covered Entity or employer
- Transmitted or maintained in any form or medium
- Identifies the individual
- Related to:
  - Physical or mental health condition (past, present or future);
  - Provision of health care; and
  - Payment for an individual's health care (past, present or future)

NOTE: Protected Health Information may be in oral, paper or electronic format.

HIPAA Workflow Diagram



HIPAA - Requirement to Safeguard PHI

HIPAA requires entities handling personal data to establish reasonable safeguards to protect PHI from improper use or disclosure

Categories of required PHI safeguards:

- Administrative safeguards
- Technical safeguards
- Physical safeguards

HIPAA Record Retention Requirements

Retain copies of documents for a period of six (6) years after the later of:

- When document is created; **or**
- When PHI is no longer in effect

Documents to be retained include:

- Health information complaints and responses
- Authorizations received
- Designation of Privacy Officer
- Health Plan documents
- Business Associate privacy agreements
- Training records

Sanctions for Noncompliance with HIPAA

HIPAA Penalties (Enforced by Office of Civil Rights)

- **Civil Penalties:** $100 per violation; up to $25,000 per year for same violation
- **Criminal Penalties:** Up to $250,000 and 10 years in prison for disclosure under false pretenses with intent to sell or use for commercial gain or malicious harm

Potential Litigation / Regulatory Exposure

Sanctions Imposed by Company Health Plans

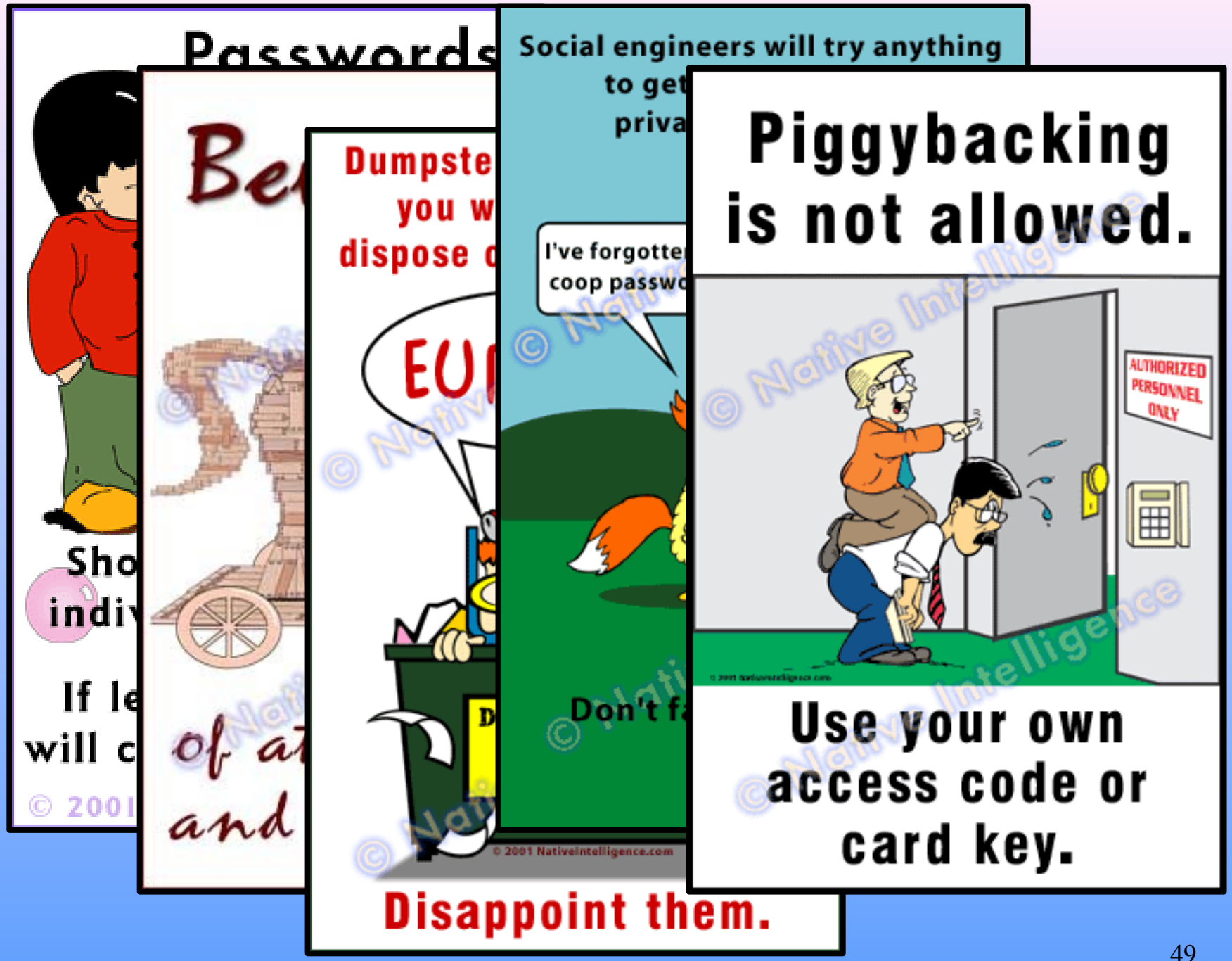
Why do I care?

What's in it for ConAgra Foods?

What is data privacy?

Why is maintaining data privacy important to me?

*What **must** I do to protect data privacy?*


Passwords
Social engineers will try anything
to get
priva
Piggybacking
is not allowed.
I've forgotte
coop passwo
AUTHORIZED
PERSONNEL
ONLY
Don't f
Use your own
access code or
card key.
Dumpste
you w
dispose
EU
© 2001 NativeIntelligence.com
Disappoint them.
Be
of at
and
Sho
indiv
If le
will c
© 2001
© Native Intelligence

Resources

- U.S. Federal Trade Commission: http://www.ftc.gov
- U.S. Federal Trade Commission Identity Theft Internet Site: http://www.consumer.gov/idtheft/
- Internet Fraud Complaint Center (IFCC): http://www1.ifccfbi.gov/index.asp
- U.S. Department of Justice Internet Fraud: http://www.usdoj.gov/criminal/fraud.html
- National Fraud Information Center: http://www.fraud.org/welcome.htm
- U.S. Securities & Exchange Commission Internet Investment Scams site: http://www.sec.gov/investor/pubs/cyberfraud.htm
- Anti-Phishing Working Group: http://www.antiphishing.org/

Questions

Why do I care?

ONLY YOU CAN PROTECT OUR DATA