INFORMANT

EDUCATIONAL INFORMATION ABOUT SAFE USE OF THE INTERNET

IDENTITY THEFT

PROTECTING YOUR BUSINESS & YOUR CUSTOMER INFORMATION

Law enforcement agencies describe identity theft as the fastest growing crime that business, consumers and governments face.

What is identity theft?

Identity theft refers to crimes in which someone wrongfully obtains and uses another person's personal data, including name, date of birth, social security number, driver's license number, and your financial information from credit cards, bank account and phone-card numbers.

How identity thieves get your information:

- **Business record theft:** by stealing files out of offices where you are a customer, employee, patient or student.
- **Shoulder Surfing:** by standing behind you in line and memorizing your information while you write a check, or punch in your phone or credit card numbers.
- **Dumpster Diving:** by rummaging through your trash or landfills.
- **Skimming:** by stealing your credit card number as your card is being processed at a restaurant, store or other business.
- **Inside job:** company employees who have access to sensitive company information and steal it for their own personal gain.

How does your company keep client information?

Most companies collect and retain client information:
- A single computer can hold thousands of client records.
- A filing cabinet may contain access codes, passwords and license numbers that are shared with partners, suppliers or vendors.
- Outside contractors manage company IT functions and databases and have access to sensitive company information.

For More Information

www.AnnualCreditReport.com
www.equifax.com
www.experian.com
www.transunion.com
www.privacyrights.org/identity.htm
www.consumeraction.gov

Securing company data and storage:

- Paper records with personal information should be locked, and computer terminals password-protected.
- Place your computer server(s) in a secure, controlled location, and keep other devices such as back-up CDs or tape drives, locked away.
- Physically lock up all laptops to prevent thieves from walking away with one.
- Keep customers and other non-authorized personnel out of private and secure areas.
- Instruct employees to save data, including databases, to network drives where these are available and not to "C" hard drives on computers.
- Prevent unauthorized photocopying of company records.
- Instruct employees to be discrete when discussing sensitive information over the phone, so that others around them won't be able to hear what they are saying.
- Properly screen and do background checks on all new and potential employees.
- Establish a company policy for handling sensitive customer information and educate all employees on the proper procedures for collecting and storing the information. Appoint one person to be in charge of implementing the procedure.

PROTECT YOURSELF & YOUR CUSTOMERS!

WHAT IDENTITY THIEVES LOOK FOR	- Name - Address - Date of Birth - Social Security No. - Driver's License No.	- Mother's maiden name - Account numbers - Card expiration dates - Internet passwords - Personal Identification No's	- User IDs for online account access - Security codes from the back of credit and debit cards	**Be sure to use a cross-cut shredder to dispose of documents containing any of the information listed at left.**

INFORMANT

EDUCATIONAL INFORMATION ABOUT SAFE USE OF THE INTERNET

~GONE PHISHING~

Internet Identity Theft

phishing (FISH.ing) *pp*. Creating a replica of an existing Web page to fool a user into submitting personal, financial, or password data. —*adj*. —**phisher** *n*.

FBI called **phishing** the "hottest, and most troubling, scam on the Internet."

What is Phishing and Pharming?

Phishing attacks steal consumers' personal identity data and financial account credentials by using 'spoofed' e-mails to lead consumers to counterfeit websites, designed to trick recipients into divulging financial data such as credit card numbers, account usernames, passwords and social security numbers. Hijacking brand names of banks, e-retailers and credit card companies, phishers often convince up to 5% of recipients to respond. Crimeware is implanted onto PCs to steal credentials directly, often using Trojan keylogger spyware. Pharming crimeware misdirects users to fraudulent sites or proxy servers, typically through DNS (domain name server) hijacking or poisoning.

How to Avoid Phishing Scams

While online banking and e-commerce is very safe, be careful giving out your personal financial information over the Internet.

- Be suspicious of any email with urgent requests to provide personal financial information or to fill out forms.
- Don't use the links in an email to get to any web page, call the company on the telephone, or log onto the website directly by typing the web address in your browser.
- Ensure that you're using a secure website when submitting credit card or other sensitive information via your web browser, URL should be https:// rather than "http://".
- Routinely log into your online accounts, including bank, credit and debit card statements to ensure that all transactions are legitimate.
- Keep your web browser up to date, Microsoft Internet Explorer users should go to http://www.microsoft.com/security/ to download a special patch relating to certain phishing schemes.
- Always report "phishing" or "spoofed" e-mails:
  - forward the email to reportphishing@antiphishing.com
  - forward the email to the Federal Trade Commission at spam@ftc.gov
  - forward the email to the "abuse" email address at the company that is being spoofed (e.g. "spoof@ebay.com")
  - when forwarding spoofed messages, always include the entire original email with its original header information intact.

Identity Theft Help Sites:
www.antiphishing.org

Identity Theft Quiz For Consumers:
www.usdoj.gov/criminal/fraud/websites/idquiz.html

Interactive e-Card:
www.ftc.gov/bcp/edu/multimedia/ecards/phishing

Just Say "NO"

- In general - no one should respond/reply to an unsolicited email message, or forward an email message to a friend, family member, or co-workers - when the email message encourages you to do so. For example: Chain e-mails encourage the recipient to forward to as many people as possible, warning them not to break the chain (see definitions at the bottom of the page on how viruses work).
- If you respond to a request to be "removed" (from the "send to" list) from an "unsolicited" message sent to you, you are notifying the sender that you have a working email account. Just delete the message.
- Never open an email attachment, unless you knew it was expected, or you speak with the sender to verify its contents. If you are unsure it is OK, delete the entire message.

Source: Anti-Phishing Working Group (APWG) - Committed to Wiping Out Internet Scams and Fraud at www.antiphishing.org.

WHAT DOES THAT MEAN?

Viruses - A virus is a small piece of software that piggybacks on real programs. Each time the program runs, the virus runs, too.

E-mail viruses - An e-mail virus moves around in e-mail messages and usually replicates itself by automatically mailing itself to all the people in the victim's e-mail address book.

Worms - A worm is a small piece of software that uses computer networks and security holes to replicate itself.

Trojan horses - A Trojan horse is a computer program, that claims to do one thing (it may claim to be a game) but instead does damage when you run it (it may erase your computer hard disk). Trojan horses have no way to replicate automatically.