



KEEP SAFE

A Monthly Publication for Texas Electric Cooperatives

May 2008

Protecting customers from identity theft

Identity theft can have devastating financial and psychological consequences for the individuals whose personal information is stolen. When thieves make purchases, empty bank accounts, or take out loans under other people's names, it can take months, or even years, for victims to restore their credit records.

Less well-known is the catastrophic effect identity theft can have on businesses that fail to adequately protect confidential data. "Losing" a customer's data can result in litigation or fines and may damage a company's reputation irreparably when a data breach is made public. Smaller companies, in particular, are at risk of being targeted by identity thieves as larger companies become more adept at warding off attacks by hackers and other thieves.

Here are some of the precautions you, as a business owner, can take to reduce the risk of sensitive customer data falling into the wrong hands:

- ◆ Minimize the amount and types of information collected. The theft of Social Security numbers can be particularly damaging to individuals, so companies should use other means of identifying customers whenever possible. Even less sensitive types of information, such as phone numbers and birth dates, can be attractive to thieves.

- ◆ Conduct all e-commerce transactions through authentication systems with several layers of security designed to verify that the user who accesses an account or provides information is the legitimate owner of that information.

- ◆ Draft a privacy policy and train employees. Firms should have a privacy policy in place with rules on the handling of customer data, and all employees with access to sensitive data should be instructed in these rules.

- ◆ Restrict employee access to data. Employees should be authorized to view or handle data on a "need-to-know" basis. There are software programs available that allow you to monitor who is accessing the data at any given point in time. Store this information in case an audit becomes necessary later. Access to the company's databases should be withdrawn immediately when an employee leaves the company.

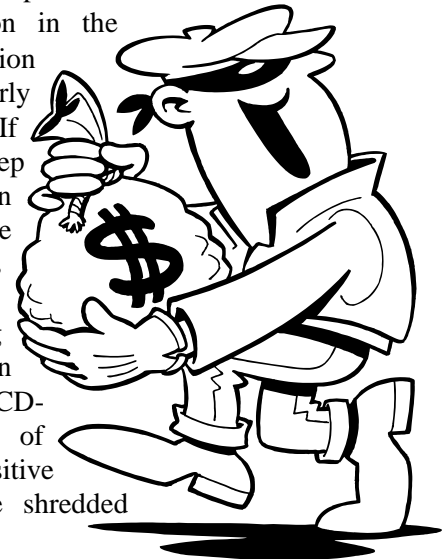
- ◆ Remind employees that phone conversations can be overheard and computer screens can be viewed by unauthorized individuals. Employees should take care when discussing confidential information and lock their PCs when they are away from their desks.

- ◆ Shield your computer network with firewalls designed to create a protective barrier between your company's network and the Internet. Available as both software or hardware, firewalls can stop potential hackers from gaining access to confidential information stored in your system.

- ◆ Use encryption when exchanging sensitive information with customers via a website or email, and encrypt confidential customer data stored on servers and backup systems. Encryption software scrambles data during transit over the Internet, making it difficult for hackers to intercept and steal.

- ◆ Install antivirus and anti-spyware software packages on all company computers. These programs should include automatic updates and should never be disabled. As an extra precaution, remind employees not to open email from unfamiliar addresses.

- ◆ Store information in the most secure location possible, and properly dispose of old records. If it is not necessary to keep customer information online, it is safer to store it offline in file cabinets under lock and key. Avoid storing confidential data on easily stolen disks or CD-ROMs. Hard copies of records containing sensitive information should be shredded when no longer needed.



(Identity theft continued on page 2)

(Identity theft continued from page 1)

◆ Protect hardware from tampering or theft. Thieves can tap into sensitive data stored on servers or the hard drives of PCs and notebooks if they find or steal the equipment. Employees should not take notebooks containing sensitive customer information outside the company unless it is necessary to do so. Businesses should run hard-drive shredding software before disposing of old computer equipment.

◆ Include as little personal information as possible in written correspondence to customers, as thieves can steal Social Security and account numbers by intercepting mail.

If a data breach nonetheless occurs, it is essential to take prompt action. The compromised accounts should be suspended immediately, and the systems containing the data should be shut down to prevent additional theft. Notify the police and the FBI of the breach, as well as any customers who might be affected. Your company's security systems should be thoroughly analyzed to establish how the breach occurred, and steps should be taken to prevent future losses.

— Vol. 14 No. 1, Risk Manager Online
© Liberty Publishing, Inc.

6 Tips for spring fitness success

1 Develop reasonable goals. If you've never run a mile, running a marathon is probably not for you yet! Start by walking one mile, then walking two. When you've walked two miles, try running one mile and so on. It's important that you don't do too much, too fast. Taking a day off between workouts is a good way to avoid overtraining and reduce the likelihood of injury.

2 Remember the 10% rule. Never increase any element of your activity by more than 10 percent per week. For example, if you swim for 20 minutes in your first week of exercise, swim 22 minutes in your second week, 25 minutes your third week, and so on.

3 Don't pick up where you left off. If you finished your exercise season in late summer by biking 20 miles, don't start your spring routine with a 20-mile trek. Build up gradually and give your body time to adapt to the increased demand.

4 Balance your workout. Include upper and lower body exercises in your workout. This helps avoid muscle imbalance and overtraining, and improves your overall fitness level.

5 Variation is the key. Adding variety to your exercise regimen will keep you from getting bored and burnt-out. Try a weekly combination of walking, running, cycling, swimming and weight-training.

— Ohio Health Dimensions

Upcoming Loss Control Schools

Troubleshooting School - (Gonzales)	May 6 - 9
Bucket Truck Operations and Digger Operations School - (Merkel)	May 13 - 14
Regulator, Recloser, Capacitor - (Quitman)	May 20 - 23
Underground School - (Gonzales)	June 9 - 13
Transformer School - (Livingston)	June 24 - 27
Troubleshooting School - (Greenville)	July 8 - 11
Hotline 1 - 4 School - (Merkel)	August 11 - 15
Metering School - (Livingston)	August 19 - 22



Keepsafe is originally published monthly by the Safety and Loss Control Department of Ohio Rural Electric Cooperatives, Inc., 6677 Busch Boulevard, Columbus, OH 43229 and reprinted by permission for Texas Electric Cooperatives, 2550 S. IH-35, Austin, Texas 78704.
Telephone: (512) 454-0311 Fax: (512) 486-6273
www.texas-ec.org