

ISSUE #8 - April 2004

1. Keystroke Recording Devices
2. US Bank - Email Scam
3. Is It Really A Credit Union?
4. San Diego State University Breach

Keystroke Recording Devices

Even at the office where you work, you need to remember to protect your personal information and keep alert.

A recent case involved an employee of a company who installed a keystroke - recording device on a workplace computer of another employee.

The employee installed the device, known as a keystroke logger, on a computer used by a secretary to a Vice President of his company in order to obtain e-mails, passwords and other information.

The employee who installed the device was fired for other reasons. Soon after, he asked a former co-worker to retrieve the key logging device, known as "Key Katcher", from the back of the computer where it was installed.

The former co-worker who was a friend of the identity thief, notified company management about the device and the company notified the FBI.

We all want to trust the people we work with and do not wish to be suspicious of our fellow employees, but you may want to check the back of your computer just to be safe or ask the I.T. department for assistance.

The number of identity theft victims continues to rise and the methods used continue to get more sophisticated.

Free Credit Reports Available On The Following Dates (As Estimated By The FTC)

December 2004 – AL, AR, CA, CO, HI, ID, MT, NV, NM, OR, UT, WA, WY

March '05 – IL, IN, IA, KS, MI, MN, MO, NE, ND, OH, SD, WI

June '05 – AL, AK, FL, GA, KT, LA, MS, OK, SC, TN, TX

September '05 – CO, DE, DC, MA, MD, MA, NH, NJ, NY, NC, PA, RI, VT, VA, WV, Puerto Rico and US territories

US Bank – Email Scam

Email scams continue to increase. Although the types of email scams change, many of them are very similar but use different corporate names.

Citibank, Pay/Pal, E-Bay and now US Bank have fraudulent emails that read:

Dear US Bank Customer,
During our regular update and verification of the Internet Banking Accounts, we could not verify your current information. Either your information has been changed or is incomplete; as a result, your access to use our services has been limited. Please update your information.

To update your account information and start using our services please click on the link below:

(They then include a hyperlink to a web page that looks like your institution, but is really a fraudulent site designed to capture your personal information).

Your financial institution should never send you an email to request you to provide them with your personal information to update their records.

If you receive an email like the above delete it from your system immediately.

Is it Really a Credit Union?

Have you heard about on-line phishing scams? (Where someone sets up a phony website to look exactly like a real company web-site and utilizes it to obtain your personal information) Just like in the previous article.

Now criminals are even trying it offline and it has affected credit unions in several states.

Criminals run an advertisement using the financial institutions name and logo with a promotion for individuals to call and open an account or to access some other service. They publish an 800 number and when you call the number they answer the phone as the institution.

It is unfortunate that this occurs and that we can no longer be sure advertisements in newspapers are legitimate.

If you see an ad and you want to purchase something from that company, call information or look them up in the yellow pages to make sure the number shown in the ad matches the number in the phone book.

It may take a little more time to research the ad and to confirm the information, but it could save you time, money and your identity if the ad turns out to be fraudulent!

SDSU Security Breach

While investigating a computer server sending spam e-mail messages, the Information Technology Security Office at San Diego State University discovered computer intruders had circumvented departmental server security and gained illegal access to a file server in the Office of Financial Aid and Scholarships.

The initial investigation revealed that the intruders had used the server for file transfers (including MP3 music files) in addition to sending spam e-mail. The illegal entry also gave the intruders the opportunity to view various Financial Aid reports stored on this server. The compromised server was not the Financial Aid database, which means the intruders did not have access to aid application or award data. However, some of the reports and files stored on this system included the names and Social Security numbers for more than 178,000 individuals.

Campus Response

The University took immediate steps to limit access when the incident was discovered and the Office of Financial Aid and Scholarships took the server off the network. There is no indication that the intruders targeted confidential information or will use it for any unlawful purpose. Nevertheless, as required by California law, the University is in the process of notifying each person whose name and Social Security number were on the system.

IDENTITY FRAUD, INC.

Engaging Solutions for Identity Protection!

www.IdentityFraud.com

Email: info@identityfraud.com

© 2002 -2004. All Rights Reserved.