ID Theft Central
Utah's Identity Theft Solution

Email Phising/Pharming

Phishing can be sophisticated or simple. In its simple forms it is not new or novel. It is as simple as the information cards you fill out at displays or information fairs. Take for example the win the free car booth you pass in the mall. In order to "win the car" you fill out a card that lists some of your personal information i.e. your name and address. This is a type of phishing and in this format is legal.

There are more complex forms of phishing that are the state of the art in crime. These are the fake web sites that pose as real web sites for banks and other financial institutions. These sites may be sent to you in an email or pop up on your computer screen when you are attempting to reach the real site. The site directs you to enter your personal information including account numbers. The information is then sent to an identity thief who uses the information to access your account before you know it.

Steps to Take Immediately - Follow each step below to help recover from the damage caused by identity theft.

Step 1:

Take these steps to minimize any damage if you suspect that you have responded to a phishing scam with personal or financial information or entered this information into a fake web site.

- Change the passwords or PINs on all your online accounts that you think could be compromised.
- If you know of any accounts that were accessed or opened fraudulently, close those accounts.
- Routinely review your bank and credit card statements monthly for unexplained charges or inquiries that you did not initiate.
- If your email was hacked, you should notify individuals in your Contacts list and inform them of the situation. Warn them not to provide money or personal information to email requests originating from the compromised email account.

Step 2: Organize Your Case

In order to help law enforcement investigate your case, and to help recover from the damage caused by an identity theft, you should:

- Keep a detailed list of all phone calls you receive or make related to your identity theft incident including name of the person you spoke with, that person's title, phone number, organization name, and what was said during the conversation.
- Make sure you keep a copy of all financial statements, police reports, affidavits, credit reports, collection letters, and all other documents related to your incident.
- Keep all loose documents in a notebook or accordion folder.
- Send all correspondence using certified mail with return receipt requested.
- Keep track of your time and any expenses you incur in the event you are given the opportunity to be reimbursed for your costs through court ordered restitution.
- Use ID Theft Central's Contact Tracking Sheet to keep track of the people you speak with regarding your identity theft incident.

Step 3: Initiate a 90 Day Fraud Alert

To help protect your personal identifying information from being used to obtain new credit by a thief, initiate a 90 Day Fraud Alert. A 90 Day Fraud Alert notifies potential credit grantors to verify your identification before extending new credit in your name.

- You only need to contact one of the three credit reporting companies to set up a Fraud Alert for all three. You will receive a free copy of your credit report from all three credit reporting companies.
- You will receive a notice of your rights as an identity theft victim.
- A 90 Day Fraud Alert stays on your file for at least 90 days and can be renewed.
- A Fraud Alert may slow down your approval process for new credit.

To place a Fraud Alert, you may be required to provide appropriate proof of your identity, which may include copies of your Social Security card, driver's license, and/or utility bills. You may cancel the fraud alerts at any time.

Experian
P.O. Box 9532
Allen, TX 75013
1-888-397-3742
www.experian.com

Equifax
P.O. Box 740250
Atlanta, GA 30374-0241
1-800-525-6285
www.equifax.com

Transunion
P.O. Box 6790
Fullerton, CA 92834-6790
1-800-680-7289
www.transunion.com

Step 4: File an identity theft report at ID Theft Central or with your local police department

Once you have confirmed the information in an email of phishing scam is being used to obtain new credit, withdraw funds from your account in your name, file a report at ID Theft Central or with your local police department.

- Report the crime at ID Theft Central.
- Contact your local police department and report the crime by calling their non-emergency number and explain to them what happened.
- Make sure your police department issues you a police report with a case number.
- You can use their police report to obtain a Consumer Credit Freeze from the credit reporting companies at no cost. You can also use the report to help clear the damage caused by the theft.

Step 5: Monitor your bank accounts and credit reports regularly

It is important that you check your bank accounts and credit reports regularly to identify illegal activity. Early detection is key to minimizing the damage that mistakes and fraudulent activity can have on your credit.

The federal FACTA law enables you to receive one free credit report per year from each of the three credit reporting agencies. These are in addition to the free reports you can order after you place a Fraud Alert on your credit file. Order your free credit reports online at www.annualcreditreport.com.

We recommend that you stagger the receipt of your credit reports, ordering one approximately every four months. Order your report from a different agency each time. That way you can review your credit report three times each year. If you see possible fraudulent activity on your credit report, file all of the appropriate reports on this web site.

You Might Also Like

Consumer Credit Freeze