



Protecting Yourself from Identify Theft

Consider this: you get an urgent e-mail from your bank saying they have detected a serious problem with your account. To fix it, they want you to log on to their website, using the secure link they have provided. Once you log on, you are directed to confirm your account number, personal identification number and password. The bank apologizes for the inconvenience, but unless they hear from you, your account will be deactivated.

If you followed these instructions, you probably saw a very official-looking website. If you confirmed all your account information, you are now a victim of identity theft. Someone went “phishing,” and by taking the bait, you joined an increasingly large group; perhaps as many as one out of every five people are identity theft victims.

“Phishing” is any fraudulent scam to get you to voluntarily disclose private personal information: financial data, account numbers, passwords, Social Security Number, account login, and the like. After you disclose it, scammers can (and do) use it to empty bank accounts, charge-up credit cards, apply for loans, and all manner of other illegal activities.

In addition to financial consequences, your credit record can be significantly harmed. And, if your credit cards are maxed-out and denied when you next go to use them, you may suffer personal and social embarrassment. You might also find yourself on the wrong side of the law if your information is used to commit a crime.

So what can you do to protect yourself from identify theft? Thankfully, there’s a lot. In the case above, immediately call your bank to report the fraudulent e-mail, ask the bank to flag your account for unusual activity, or even cancel your account and open a new one; and ask your bank to notify you if accounts are opened in your name without your permission. Legitimate financial and government organizations will almost never use e-mail to ask you for private, personal

information. They will likely send a letter, at which point you can call the institution to determine what's going on.

If you have given out this kind of personal information to a phisher, the Federal Trade Commission (FTC) recommends that you report the theft to the three major credit reporting agencies, Experian, Equifax and TransUnion Corporation, and request that they place a fraud alert and a victim's statement in your file:

- Experian: 1-888-EXPERIAN (1-888-397-3742), www.experian.com
- Equifax: 1-800-525-6285, www.equifax.com
- Transunion: 1-800-680-7289, www.transunion.com

If an identify thief is opening new credit accounts in your name, they are likely to show up on your credit report. You may catch an incident early if you order a *free* copy of your credit report periodically from any of the three major credit bureaus. The FTC also recommends that you review credit card and bank account statements as soon as you receive them to check for unauthorized charges, and use anti-virus software and a firewall, and keep them up to date. Above all, be aware and ask questions before responding to unsolicited emails or other requests for information.

If you believe you've been scammed, file a complaint with the FTC at <http://www.ftc.gov>.

Additional information:

www.antiphishing.org or www.phishinginfo.org. Information from the National Consumers League)

<http://www.ftc.gov/bcp/online/pubs/alerts/phishingalrt.htm>. Federal Trade Commission (FTC) article on "How Not to Get Hooked by a 'Phishing' Scam"

Cathy Rosebaugh is a Certified Senior Advisor and Seniors Real Estate Specialist with Alterna Home Solutions. If you have questions about this article, please contact Cathy at 919-460-1061.

###