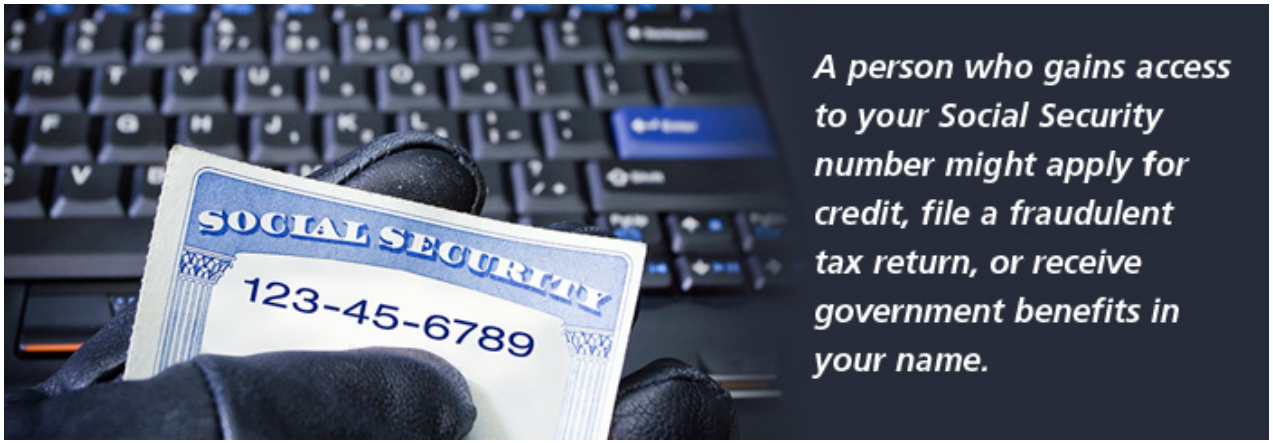
Cybercrime Update: Tips to Help Protect Your Money, Privacy, and Identity

Federal prosecutors recently indicted members of an alleged gang of cyber thieves for stealing $45 million from banks in coordinated global attacks, each of which lasted only several hours. Sophisticated hacking techniques were used to remove spending limits on prepaid debit-card accounts at two banks in the Middle East. Organized crime cells then programmed corresponding debit cards to withdraw money from bank ATMs around the world, including $2.8 million from nearly 3,000 ATMs in New York City in two separate attacks that took place in December 2012 and February 2013.[1]

The heist is believed to be the second-largest global bank robbery on record. In New York City, the bank theft was second only to the 1978 Lufthansa robbery depicted in the movie “Goodfellas.”[2]

News of such brazen and costly attacks demonstrates how difficult it can be for individuals, businesses, and governments to detect the latest cyber threats and protect their interests. Unfortunately, millions of American consumers could become victims of cybercrimes such as debit- or credit-card fraud and identity theft each year.

Here’s a closer look at common cybercrimes that could affect you, as well as steps to help safeguard your personal information and financial accounts.



Compromised Accounts

It has become increasingly common for criminals to install “skimmers” that collect the data embedded in the magnetic strip on the back of credit and debit cards. The electronic devices are placed on ATMs, inside gas pumps, or at other retail establishments where cards are swiped, and they may be used in conjunction with small cameras that capture the cardholders’ PIN numbers.

Cloned cards can then be used to make purchases or steal cash until the account is frozen by the bank. In many cases, victims may not realize that “skimming” has occurred until fraudulent transactions appear on their accounts or they are contacted by the bank.

Before swiping your card at an ATM or a gas station, inspect the machine and look closely at the card slot to detect a skimmer. When you enter your PIN, cover your hand to prevent a camera from recording your number.

To help limit the hassles and potential losses of a cybercrime, monitor your accounts regularly and notify your bank immediately if you notice any suspicious activity. Stolen funds are typically returned to customers when claims of fraud are filed promptly. The U.S. Secret Service estimates that ATM skimming is responsible for more than $1 billion in losses on an annual basis.[3]

Identity Theft Persists

Identity theft is not a new problem, but criminals continue to devise sinister schemes to steal personal information and cash in after they have it. About 12.6 million people had their identities stolen in 2012.[4]

Cyber thieves are not only after your existing financial accounts. A person who gains access to your Social Security number might apply for credit, file a fraudulent tax return, or receive government benefits in your name.

Phishing schemes are spam emails that try to trick you into giving your personal information or log-in credentials to computer hackers. At first glance, a sophisticated attempt may look as though it was sent from your own bank or a company you do business with. However, legitimate businesses generally won’t ask you to provide sensitive data via email.

Don’t Leave a Paper Trail

Keep important records (including your Social Security card) in a locked drawer at home. If you have a Medicare card, carry only a copy of it with all but the last four digits blacked out. Shred documents or cards instead of throwing them in the trash.

Send outgoing mail from an official or locked mailbox. When you are out of town, have the postal service hold your mail or ask a friend to pick it up.

Be Cautious Online

To help thwart hackers, create strong passwords with a combination of uppercase and lowercase letters, numbers, and special characters. Use a separate password for every account, and don’t use an automatic log-in feature that saves your username and password. Never enter personal data on a public computer unless you can log in and out of a secure account.

Enter sensitive data only on encrypted sites that display a “lock” icon on the status bar of your Internet browser. Mobile devices may also be vulnerable, so it’s important to enable the encryption and password features on your smartphone.

For more information about online security issues and consumer scams (compiled by a coalition of government and consumer protection agencies), visit *OnGuardOnline.gov.*

1–2) CNNMoney, May 9, 2013
3) Yahoo! Finance, May 3, 2013
4) *Kiplinger’s Personal Finance*, June 2013

The information in this article is not intended as tax or legal advice, and it may not be relied on for the purpose of avoiding any federal tax penalties. You are encouraged to seek tax or legal advice from an independent professional advisor. The

content is derived from sources believed to be accurate. Neither the information presented nor any opinion expressed constitutes a solicitation for the purchase or sale of any security. This material was written and prepared by Emerald.
Copyright © 2013 Emerald Connect, Inc.

Portal | Focus Financial

Physical: 650 S. Cherokee, Suite F • Catoosa, OK • 74015
Mailing: PO Box 550
Phone: 918-266-2787 • Fax: 918-266-2793
portal.myfocusteam.com • info@myfocusteam.com

print this page

Securities offered through **GWN Securities, Inc.,** Member FINRA and SIPC

11440 N Jog Road, Palm Beach Gardens, FL 33418, 561-472-2700.

Focus Financial and GWN Securities, Inc are non-affiliated companies.

Privacy Policy