Atlantic County Sheriff's Office Wishes you a Happy New Year!

JANUARY 2013

Protect yourself from Identity Theft in 2013

Three Things You Need to Know if You Use Online Banking

Banks are well aware that criminals will use any trick they can to get control of your money. To stay ahead of the cat and mouse game, financial institutions use one-time passwords and verification codes that render most conventional phishing attacks useless. Thus online criminals have had to innovate quickly.

Man-in-the-middle attack allows the attacker to intercept messages between you and your bank. The criminal then sends its own messages to both parties. Recently, there have been multiple man-in-the-middle attacks against at least two east coast banks. Other new man-in-the-middle attacks utilize the computing power of our smartphones to trick us out of account information.

1. **Never click on links from bank e-mails.**
   When you're busy, it's easy to make a mistake and click on a bad link, especially on our phones. Sean Sullivan from F-Secure Labs says the best strategy is to, "Go to the bank via a browser bookmark."

2. **Know that criminals are targeting your smartphone.**
   F-Secure Labs has followed Spitmo, a man-in-the-middle attack that targets phones, since spring. And now an Android version has been spotted. This attack pretends to install an application that protects the phone's SMS messages. If you receive an SMS that asks you to install such Software on your phone, take the time to contact your bank directly.

3. **Keep your system and security software updated.**
   The registered owner of a site which has been linked to a bank attack owns more than 90 sites. So as one attack goes down, another one might go up. It's important to have browsing protection that could prevent you from visiting a site hosting a known attack. And it's even more important to make sure your PC is protected.

Criminals will never stop scheming of ways to get into your bank account. By staying aware of their latest tricks, you'll do your best to keep your money where it belongs.

Inside this issue:

The Atlantic County Sheriff's Office newsletter is designed to inform you of what's new at ACSO, as well as point out some safety tips to help keep you and your family safe.

Frank Balles

Atlantic County Sheriff

Smishing & Vishing: And Other Cyber Scams

Scenerio: You receive a text message or an automated phone call on your cell phone saying there's a problem with your bank account. You're given a phone number to call or a website to log into and asked to provide personal identifiable information-like a bank account number, PIN, or credit card number-to fix the problem.

But beware: It could be a **"smishing"** or **"vishing"** scam….and criminals on the other end of the phone or website could be attempting to collect your personal information in order to help themselves with your money. While most cyber scams target your computer, smishing and vishing scams target your mobile phone, and they're becoming a growing threat as a growing number of Americans own mobile phones (Vishing scams also target landline phones).

"Smishing"-a combination of SMS texting and phishing-and "Vishing"-voice and phishing– are two of the scams the FBI Internet Crimes Complaint Center (IC3) is warning consumers about. These scams are also a reminder that cyber crimes aren't just for computers anymore.

Here's how smishing and vishing scams work: criminals set up an automated dialing system to text or call people in a particular region or area code (or sometimes they use stolen customer phone numbers from banks or credit unions). The victims receive messages like: "There's a problem with your account," or "Your ATM card needs to be reactivated," and are directed to a phone number or website asking for personal information. Armed with that information, criminals can steal from victims' bank accounts, charge purchases on their charge cards, create phony ATM card, etc.

"While most cyber scams target your computer, smishing and vishing scams target your mobile phone"

Sometimes if a victim logs onto one of the phony websites with a smartphone, they could also end up downloading malicious software that could give criminals access to anything on the phone. With the growth of mobile banking and the ability to conduct financial transactions online, smishing and vishing attacks may become even more attractive and lucrative for cyber criminals

Here are a couple of recent smishing case examples:

- Account holders at one particular credit union, after receiving a text about an account problem, called the phone number in the text, gave out their personal information, and had money withdrawn from their bank accounts within 10 minutes of their calls.
- Customers at a bank received a text saying they needed to reactivate their ATM card. Some called the phone number in the text and were prompted to provide their ATM card number, PIN, and expiration date. Thousands of fraudulent withdrawals followed.

Other cyber scams to watch out for, according to IC3 include:

- Phishing schemes using e-mails that direct victims to spoofed merchant websites misleading them into providing personal information.
- Online auction and classified ad fraud, where Internet criminals post products they don't have but charge the consumer's credit card anyway and pocket that money.
- Delivery fraud, where online criminals posing as legitimate delivery services offer reduced of free shipping labels for a fee. When the customer tries to ship a package using a phony label, the legitimate delivery service flags it and requests payment from the customer.
- Don't respond to text or automated voice messages from unknown or blocked numbers.
- Treat your mobile device like your computer-Don't download anything from an untrusted source.
- When buying online, use a legitimate payment service and use your credit card. You can dispute charges on your credit card.
- Don't respond to unsolicited e-mails, texts, or phone calls requesting personal information.

For more information about the latest cyber crime scams, visit IC3's website.

Scam Watch: Child Identity Theft, Credit Repair, Investments

Here is a roundup of alleged cons, frauds and schemes to watch out for.

Child identity theft—Scammers have increasingly been using children's social security numbers to steal their identities and establish fraudulent credit cards and loans, the Better Business Bureau said in a recent bulletin. In one instance, a 17 yr. old girl's personal information was used to run up $725,000 in fraudulent debt, much of which had gone into collection, the group said. Parents should encourage children to keep their personal information secure, according to Carrie A. Hurt, president of a Better Business Bureau office that serves central, coastal and southwest Texas. Anyone concerned about their children's credit can run a check with one of the large credit-reporting agencies.

Credit repair operators— The Federal Trade Commission has filed a lawsuit accusing operators of a credit repair company of unlawfully charging fees before performing services. The lawsuit against RMCN Credit Services Inc. is part of a continuing crackdown on credit-repair companies that prey on people with financial problems, the FTC said in a news release. RMCN charged a retainer fee of up to $2,000, violating a federal law that prohibits such agencies from collecting fees without performing any services.

Investment Fraud— A man who stole "at least $1 million" from investors has pleaded guilty to wire fraud and tax evasion, federal prosecutors in New Jersey said, Robert Schroy, who lived alternately in Illinois and California, told investors he would use their money in "international bank trade" but actually spent of it on personal expenses, including cars, vacations and dining, the U.S. attorney's office in Trenton, N.J., said in a news release. Schroy and his unidentified partners promised investors extraordinary gains—ranging from 10% to 100% per week for 25 weeks, plus the return of their original investments. Unfortunately, he never invested the money, prosecutors said. The charges carry a maximum sentence of 25 years in federal prison.

"Scammers have increasingly been using children's social security numbers to steal their identities and establish fraudulent credit cards and loans"

Preventing Identity Theft: The Do's & Don'ts for Preventing Identity Theft

DO:

- Order a copy of your credit report every year from all three of the major credit reporting agencies in order to check for fraudulent activity or discrepancies. I the State of New Jersey, you can obtain one free report each year from each of the credit reporting agencies. Consider using a locked mailbox.
- Protect your mail by removing it from your mailbox as soon as possible. Consider using a locked mailbox.
- Shred any discarded paperwork that contains personal identifiers or financial information, including pre-approved credit card and loan applications. If a vendor uses carbon copies for credit card bills, ask for and destroy the carbons.
- Stop pre-approved credit offers by calling the Credit Reporting Industry at 1-888-567-8688.
- Know where your personal information is kept, who has access to it, and who you may have provided it to in the past. Protect your wallet and purse and never leave them unattended. Keep an eye on your credit card when using it to pay for purchases.
- Be aware of your surroundings when using ATM cards, making credit card purchases, using telephone credit card numbers and utilizing pin numbers or passwords.
- Carefully review your bills, bank statements, credit card statements and other financial accounts, to ensure that all balances and receipts match and no activity is unaccounted for.
- If you use a computer, install virus protection and firewall software to discourage hackers. Be aware of personal information that you send over the internet that could be viewed by others.
- Request your financial institutions to add security to your accounts, such as a special password.

Preventing Identity Theft– Do's and Don'ts Contd.

Don't:

- Do not give out personal identifiers or financial identifiers in response to unsolicited offers by mail, phone, internet, and/or in person. Identity thieves frequently pose as legitimate business people, charity workers, or law enforcement to gain your trust.
- Do not fill out personal information on warranty cards and sweepstakes entries; it is often sold to others as a marketing tool.
- Do not provide or use your social security number unless you have to.
- Do not provide personal identifiers, account numbers or other personal information unless you know the information will be secure.

Following these steps will reduce your risk of being a victim of an identity theft. Your goal should be to reduce other people's access to your information.

Important Phone Numbers and Websites :

Credit Bureaus

Equifax	Experian	Trans Union
P.O. Box 105873	P.O. Box 949	P.O. Box 390
Atlanta, Georgia, 30348-5873	Allen, Tx, 75013-0949	Springfield, Pa, 19064-0390
Credit Report: 1-800-997-2493	Credit Report: 1-888-397-3741	Credit Report: 1-800-916-8800
Fraud Alert: 1-800-525-6285	Fraud Alert: 1-888-397-3742	Fraud Alert: 1-800-680-7289
www.equifax.com	www.experian.com	www.tuc.com

Federal Trade Commision (FTC): TO file a report—www.consumer.gov/idtheft or by phone 1-877-ID-THEFT

Stolen Checks: Report it to your bank and close accounts. Set up new accounts and put stop payments on the fraudulent checks. Report the stolen checks to the check verification companies**.**

National Check Fraud Service : 1-843-571-2143
SCAN: 1-800-262-7771
TeleCheck: 1-800-710-9898
CheckRite: 1-800-766-2748
CrossCheck: 1-707-586-0551
Equifax Check Systems: 1-800-437-5120
International Check Services: 1-800-526-5380

Atlantic County Sheriff's Office
Civil Courthouse
1201 Bacharach Blvd.
Atlantic City, NJ 08401
(609) 909-7200
(609) 909-7292

Atlantic County Sheriff's Office
Criminal Courthouse
4997 Unami Blvd.
Mays Landing, N.J. 08330
(609)-909-7200
(609)-909-7292 FAX