

Individual Account takeover & Payments Fraud

What is happening now?

Version 1

What's Individual Account Takeover?

- Individual Account Takeover is a type of identity theft in which a criminal entity steals a valid online banking credentials. Small to mid-sized businesses remain the primary target of criminals, but any person can fall victim to these crimes.
- Attacks today are typically perpetrated quietly by the introduction of malware through a simple email or infected website. For a personal computer that has low resistance to such methods of attack, the malware introduced onto its system may remain undetected for weeks or even months.

Security Notice

Please be aware that some malware (computer viruses) may attempt to capture your user name and passwords. If you receive a message that the bank's systems are down, please call either Meggan Neese or Jerry Siegel at the numbers below immediately so that we can confirm if there is an issue.

Additionally, other malware may ask you to input various information to allow the bank to update your records, including your date of birth, SSN/EIN, etc., the system may then tell you to expect a phone call from the bank. If you see a screen or receive a call requesting this information, please do not provide it and call either Meggan Neese or Jerry Siegel at the numbers below immediately.

If you do need to reach the bank concerning suspicious activity, please call us instead of using email. If your computer system has been compromised, the hacker could have access to your email and delete messages before we can receive them or send fake messages authorizing various activity.

As always, if you are ever concerned about any electronic banking security issue, please do not hesitate to call us.

Meggan Neese: 334-887-2723

Jerry Siegel: 334-887-2786

Also, if the call is urgent please feel free to 0 out of Voice Mail and ask the operator to find someone.

Am I protected?

- Consumers enjoy a certain level of protection that business bank accounts, DBA's, and Estates do not, and it's called "Regulation E."
- For more information on REG E please visit one of our branches for a brochure or fdic.gov

- **Malware**-short for malicious code
Designed to disrupt and/or deny operation, gather information, and gain unauthorized access
 - Viruses- A computer virus is a computer program that can replicate itself and spread from one computer to another.
 - Worms-A computer worm is a standalone malware computer program that replicates itself in order to spread to other computers.
 - Trojan Horses-A Trojan horse, or Trojan, is a program with a benign capability that conceals another malicious program.
 - Spyware-Spyware is a type of malware (malicious software) installed on computers that collects information about users without their knowledge.
 - Rootkits-A rootkit is a stealthy type of malicious software (malware) designed to hide the existence of certain processes or programs from normal methods of detection and enable continued privileged access to a computer.

Threats-Events

- 2007 <5M
- 2009 @ 40M
- 2010 @60M

How are breaches occurring

- Hacking 81%-Hacking means finding out weaknesses in a computer or computer network and exploiting them, though the term can also refer to someone with an advanced understanding of computers and computer networks.
- Malware 69%-Malware, short for malicious software, is software designed to disrupt computer operation, gather sensitive information, or gain unauthorized access to computer systems.
- Physical attacks 10%- When attackers are able to physically access a system
- Social tactics 7 %-Manipulating people into performing actions or divulging confidential information. While it is similar to a confidence trick or simple fraud, it is typically trickery or deception for the purpose of information gathering, fraud, or computer system access; in most cases the attacker never comes face-to-face with the victims.
- Privilege misuse 5% - Abusing access rights fraud is committed by trusted users

Forget 9-5!

Wake up, have some coffee, begin the day with a nice compiled list of computer addresses for vulnerable devices along with exact user names and passwords needed to access them. After that, put in a few hours cramming malware onto selected systems, revisit last weeks victims to collect some captured data, and then head home early to the wife and kids.

What is the Info Worth?

- Credit card details \$2-\$90
- Physical credit card \$190+
- Bank credentials \$80-\$700

Security

AuburnBank maintains layered security methods in addition to your user name and password including: Fraud detection monitoring systems, challenge questions, bill pay limits and bank approval of new users and changes in user settings.

AuburnBank will never ask you for your password

What can I do?

While AuburnBank takes multiple security measures to help protect your personal information unfortunately fraud is constantly changing. Here's some tips on how to protect your sensitive information.

- **We encourage you not to communicate sensitive information through an unsecure method**
- **Reconcile accounts online monthly; at a minimum.**
- **Be very skeptical of random pop-up windows, error messages and attachments**
- **Use appropriate tools to prevent and deter unauthorized access to your network and periodically review such tools to ensure they are up to date. These tools include:**
 - **o Personal Firewalls**
 - **o Security suites**
 - **o Anti-malware, and anti-spyware programs**

Resources

Additional information can be found at

<http://www.fbi.gov/about-us/investigate/cyber/cyber>

<http://onguardonline.gov/>

Contact information

Please make sure that we have a valid email address, phone number, fax number or any other information we may need to contact you in the event we suspect unusual activity

Questions



Please feel free to contact AuburnBank if you have any questions or would like additional information on identity theft.

Contacts

Jerry Siegel - jsiegel@auburnbank.com

Meggan Neese- mneese@auburnbank.com

334-821-9200