Online Banking Security

Best Practices for Small Business

Presented by:

Andrew J. Grover, CPA, CFE, CISA
Vice President of Risk Management
Androscoggin Bank

Small Business Fraud and Theft

Home > Security > Cybercrime and Hacking

News

IT contractor gets five years for $2M credit union theft

Insider threat case the second this week, following Terry Childs guilty verdict

By Jaikumar Vijayan
April 29, 2010 08:44 PM ET

Comments (3) Recommended (9) Share

Computerworld - For the second time this week, companies are getting a stark reminder of the danger posed to enterprise networks and assets by insiders with privileged access.

DNS Perspective

April 23, 2010

Cybercriminals Attacking SMBs through ACH Fraud

By Michael Dinan, TMCnet Editor

Small- and medium-sized businesses are facing a major cybersecurity threat involving ACH fraud, an expert in the field told TMCnet during an interview that forms part of an article that appears in a special technology section of the Chicago Tribune today.

Cybercrime Poses New Risks in Commercial Banking

Richard Raysman and Peter Brown
New York Law Journal
April 14, 2010

Print Share Email Reprints & Permissions Post a Comment

A recent report calculated that small and medium-sized businesses and local government institutions are losing, on average, $100,000 to $200,000 per day to cybercriminals who perpetrate fraudulent electronic funds transfers. Typically, thieves send targeted phishing e-mails that trick users into disclosing banking log-in information or installing password-stealing malware that records their keystrokes and online banking credentials.

How do they do it?

- One real example of theft:

May 7: an unknown third party originated an ACH (Automated Clearing House) transfer from an IP address that a Maine company had never used before.

Perpetrator logged in using a Company employee's user name and password. They also successfully answered 2 challenge questions to initiate the transfer.

Krebs, Brian, "Maine Firm Sues Bank After $588,000 Cyber Heist", www.washingtonpost.com, September 23, 2009

How do they do it?

- One real example of theft:

  By May 15: Six batches totaling $588,851 were transferred to several individuals with whom Company had never done business. The batches ranged from $56,594 to $115,620. Portions of the ACH never reached its destination.

Krebs, Brian, “Maine Firm Sues Bank After $588,000 Cyber Heist”, www.washingtonpost.com, September 23, 2009

Other important factors of the story:

- ACH transfers only used for weekly payroll on Fridays.
- Account used to fund ACH transfers was tied into a line of credit that had automatic draws. No prior notice or approval was required.
- Fraud was discovered days later, when an owner received a letter, mailed to his house, stating that portions of a recent ACH transaction had been rejected due to invalid account numbers.

Krebs, Brian, "Maine Firm Sues Bank After $588,000 Cyber Heist", www.washingtonpost.com, September 23, 2009

What is ACH?
And can this happen on any account?

Krebs, Brian, “Maine Firm Sues Bank After $588,000 Cyber Heist”, www.washingtonpost.com, September 23, 2009

Key Logging Access

- Frauds typically through a “key logger” virus.
- The virus can be unknowingly downloaded from various sources.
- All keystrokes are logged and transmitted to a cyber thief.
- Using keystroke data, the thief can answer your username, password, challenge questions, PINs, etc.
- Thieves access your bank accounts and send transfer funds to “money mules”.
- “Money mules” are everyday people; hired to accept electronic funds and forward them to companies and individuals.

How to defend yourself

- Awareness of the danger.
- Best practices in business computing.
- Choose a financial institution that educates customers and users about the dangers.

How to defend yourself

- Physical security of computers
  - Know who has access to the online banking computer.
- Network security
  - Firewall protection
  - Virus protection
- Internet and E-mail practices
  - Know what is being downloaded on your online banking computer
  - Set guidelines for employees using online banking computers
- Insurance
- Internal procedures
- Financial institution security & policy
  - Know your financial institution's policy for fraud on business accounts
- Authentication
  - Multifactor Authentication

Physical Security

- Consider a dedicated computer
  - Not networked to your company data
  - Do not allow e-mail or internet surfing
  - Consider removing the ability to write to the hard drive.
  - Turn-off when not in use.

Network Security

- Firewall
  - Work with a computer firewall expert to implement and understand firewall protection for your networks and computers.
- Anti-virus protection
  - Definition files should be updated at least weekly or whenever a major outbreak of a virus occurs.
  - Continuously running in the background.
  - Full system scan should be performed after a definition update.

http://csrc.nist.gov/publications/nistpubs/800-42/NIST-SP800-42.pdf

Internet & E-mail Security

- Avoid accessing unknown Web sites
- Don’t click on hyperlinks sent via e-mail unless you are sure they are legit. Your financial institution should never ask you to click on a hyperlink to provide information.
- Go directly to the institutions Web site to log-on.
- Don’t open e-cards or other attachments that are not absolutely verified by you.
- Do not participate in Facebook games or other social networking apps on your business computer.

Insurance

- Losses from cyber crimes are not typically covered by general or liability insurance.
- Consider insurance specific to cyber crime.
- Understand your coverage and your exposure.

Internal Procedures

- Review your activity frequently.
  - On-line banking allows for increased monitoring.
- Use ACH only if you need it.
  - Most small businesses can use online bill pay which is different than ACH and more difficult to defraud in large sums.
  - If you use ACH, work with your Bank to fully understand the risks and best security practices.
- Strong Multi-factor authentication

Authentication

- Something you are (Biometrics)
  - Voice
  - Fingerprint
- Something you know
  - User Name
  - Password
  - PIN
- Something you have
  - Token
  - USB plug
  - Smart card

Multifactor Authentication

- One form of authentication is not strong enough
- Biometrics is the strongest; however very expensive to implement
- User names, passwords, PINs are not strong enough by themselves
- Challenge questions can be “adequate” at best; however, they are often considered a weak control, based on implementation.
- Combining more than one of the methods of authentication mentioned
- Currently, one of the strongest methods of multifactor authentication is combining username, password with token technology

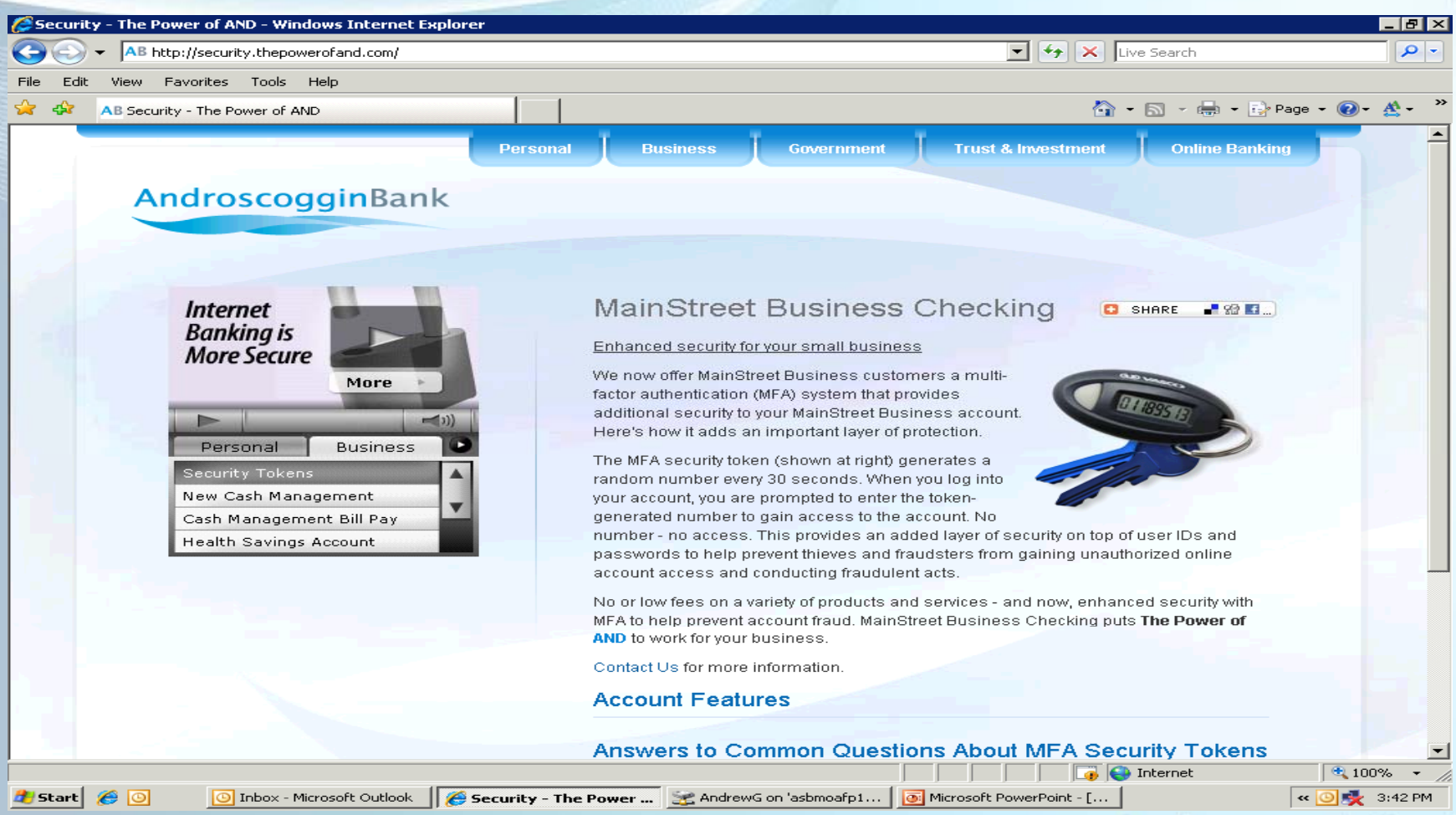
What are Tokens

- A small device that creates a random six or eight digit number
- The number changes every 30 to 60 seconds
- The random number is synced with your login
- Token is specific to a user, cannot be shared or duplicated

Using Tokens: Security Alerts

- Beware of e-mail requesting token information
  - Tokens are for you to either log into a site or conduct a transaction, only
  - Financial institutions will never request this information in an e-mail or otherwise

For more information:
visit http://security.thepowerofand.com/



AndroscogginBank

The Power of AND.

Questions or Comments

Andrew J. Grover, CPA, CFE, CISA

Risk Management
30 Lisbon Street
Lewiston, Maine 04243
Office Phone: 207-784-9164
e-mail: agrover@androscogginbank.com