

Get the edge.



# Online Fraud

## How to Protect Your Small Business

November 12, 2009

### Account Compromising and Fraud



Recently, The Financial Services Information Sharing and Analysis Center (FS-ISAC) had released an article on the topic of Account Hijacking of Corporate Customers and Recommendations for Customer Education. Below are some highlighted points.

**Compromise**—Typically compromise of the customer involves a “spear phishing” e-mail which directly names the recipient correctly and contains either an infected file or a link to an infectious Web site. Once the user opens the attachment, or clicks the link to open the Web site, malware is installed on the user’s computer which usually consists of a Trojan keystroke logger, which harvests the user’s corporate online banking credentials.

**Fraud**—The customer’s online credentials are either uploaded to a website from where the fraudster can later download them, or, if the bank and customer are using two factor authentication system, the Trojan keystroke logger may detect this and immediately send an instant message to the fraudster alerting them of the secure web activity. The fraudster then accesses the financial institution through use of the captured username and password or through hijacking the secure web session. The fraud is carried out when the fraudster creates another user account from the stolen credentials or directly initiates a funds transfer masquerading as the legitimate user. These transfers have occurred through wire or ACH that are directed to the bank accounts of willing or unaware individuals. Often within a couple days, or even hours of recruiting money mules and opening accounts, money is deposited and the mule is directed to immediately forward a portion of the money to subjects in Eastern Europe by various means.

#### Additional Information:

Community National Bank will never ask you for your Passwords, User ID’s ...etc in an email.

If you think your banking information was compromised, call CNB immediately in order for us to take appropriate action in removing online banking capabilities.

To file an incident; The Financial Services Information Sharing and Analysis Center, Inc. urges customers to contact their local FBI field office, <http://www.fbi.gov/contact/fo/fo.htm>, or file a complaint online at [www.IC3.gov](http://www.IC3.gov)

### Steps To Protect Your Small Business

- Reconciliation of all banking transactions on a daily basis.
- Initiate ACH and wire transfer payments under dual control, with a transaction originator and a separate transaction authorizer.
- Employ best practices to secure computer systems in their business including but not limited to:
  - Carry out all online banking activities from a stand-alone, hardened and completely locked down computer system from which e-mail and Web browsing are not possible.
  - Be suspicious of e-mails purporting to be from a financial institution, government department or other agency requesting account information, account verification or banking access credentials such as usernames, passwords, PIN codes and similar information. Opening file attachments or clicking on web links in suspicious emails could expose the system to malicious code that could hijack their computer.
  - Install a dedicated, actively managed firewall, especially if they have a broadband or dedicated connection to the Internet, such as DSL or cable. A firewall limits the potential for unauthorized access to a network and computers.
  - Create a strong password with at least 10 characters that include a combination of mixed case letters, numbers and special characters.
  - Prohibit the use of “shared” usernames and passwords for online banking systems.
  - Consider installing spyware detection programs.
  - Limit administrative rights on users’ workstations to help prevent the inadvertent downloading of malware or other viruses.
  - Never access financial services information at Internet cafes, public libraries, etc. Unauthorized software may have been installed to trap account number and sign on information leaving the customer vulnerable to possible fraud.

