Online Banking Fraud Prevention

July 10, 2008

Ideas
to reach your goals.

Advice
to make your decisions with more confidence.

Solutions
to meet your challenges with greater ease.

Help Protect Your Company From Online Fraud

The Federal Trade Commission estimates that identity theft costs U.S. consumers and businesses more than $50 billion a year. Perpetrators have been able to assume the identity of a legitimate corporation and use it to establish credit card accounts, set up fake subsidiaries and even lure customers into giving out their company's online banking credentials. Because the financial services industry plays a critical role in the operation of most businesses, it's important that banks commit to enhancing online security to help protect their customers.

Although federal guidelines require banks to make online authentication complex, there are still some steps you can take to help protect your own company from fraud.

- Running the most current anti-virus and anti-spyware software is a quick and easy way to protect your financial information. Talk to your IT team to make sure your company has the right protection and that it is updated routinely
- There are several services offered by banks to help prevent fraud. Our Positive Pay service compares your company's version of issued checks with checks that have come into the bank for payment and flags any that are unmatched. You can then review any suspect checks online and instruct PNC to either pay or return them. Reviewing balance and transaction information daily will not only give you a true picture of your cash flow, but can help you to identify unauthorized transactions quickly.
- Take advantage of convenient, online security tools within the bank's online banking platform. PNC's Pinacle allows customers to manage all of their treasury activities and put specific security measures in place. For example, you can set a dollar limit per user and per day on funds transfers or ensure that actions taken by your online banking administrator cannot be completed without a second adminstrator's approval. Pinacle also provides helpful information about user activity such as a "last login date and time" on the home page, audit logs and a failed login report. Monitoring this information

Lynn Nettleton
Group Product Manager
PNC Treasury Management
(412) 762-6018
lynn.nettleton@pnc.com

may help you detect attempts at fraud.

- The next suggestion is one we've all heard before. Don't write your passwords down or store them anywhere on your computer. Encourage employees to do the same. We'll prompt you to change your PINACLE password regularly, but you can change it yourself as frequently as you wish. Remember it's best to use a random combination of numbers and letters for them. Don't use birthdays or addresses or anything else that might be common knowledge.
- Don't conduct business transactions from a public or shared computer. It's also smart not to try and view your company's financials or transfer funds if you're working remotely on an unsecured wireless network.
- It's pretty common to get e-mails with links in them. A lot of companies, including PNC, use links to direct customers to websites as a way of sharing information. We suggest that you don't click on links in e-mails unless it's an email you expected to receive from a trusted source. And never enter confidential information on a web page that you reached from one of those links. It's best to go directly to a web page by typing the URL directly into your browser.

Keep all of your employees updated on potential threats or new tools you may be using to prevent online identity theft. If they're aware of the risks and how they can play a part in preventing security breaches, they'll be more willing to take the steps necessary to protect your company's information.

As criminals' methods for obtaining IDs and passwords become even more sophisticated, banks will continue to develop new tools to help protect your company's accounts from unauthorized activity. For more information about online authentication tools such as tokens, security questions or digital certificates please contact me or your PNC relationship manager. Thanks for watching.

CIB-PDF-0708-12

PNC