

Online Fraud Awareness and Prevention – Business e-Cash Manager

What You Should Know

It is more critical than ever that users of online services be aware of fraud and stay informed about how to protect against it. The financial services industry, which makes up 92.6% of the industries targeted, has seen sharp escalation in fraudulent activity. The Anti-Phishing Working Group, an industry monitoring group, reports an 89.8% increase in online fraud attempts between August 2005 and August 2006. By understanding the common approaches used to commit fraud, users of online banking services can take the steps necessary to protect themselves. Below is information you should be aware of:

What to Look Out For

Phishing involves the use of fraudulent emails or pop-up Web pages that appear legitimate and are designed to deceive a user into sharing personal or account information. This may take the form of an email notifying you of a change to your account, such as an update to your email address or change of password, or to notify you of a required software upgrade. The message may include a link to a site that looks legitimate and prompts you to enter information such as a user ID and password, which is then collected through the site.

Pharming occurs when hackers manipulate Internet mapping so that when you type in a legitimate Web address, you are redirected to a fraudulent Web site without your knowledge or consent. The Web site will look similar to the legitimate site in hopes of capturing confidential information.

Spyware is malicious software that can be loaded on your computer without your knowledge and used to capture user IDs and passwords as you access Web sites. To see common fraud examples and keep informed, visit our Web site.

What You Can Do

- Do not respond to phishing emails.**
- Look beyond the logo.** Scammers often use actual logos and corporate imagery on their sites. They also press you to provide, update or verify account information claiming access to your accounts will be suspended if you don't comply.

- Use your spam filter.** Spam filters minimize the amount of spam you receive thereby reducing the number of fraudulent emails in your inbox.
- Type, don't click.** If you do open a suspicious email, don't click on any links because you could unknowingly download a virus or spyware to your computer. Even if you think the email is legitimate, type Web addresses into your browser or use a bookmark you have created instead of clicking on links.
- Never share passwords.** Always maintain the confidentiality of your passwords, PINs and other personal information required to access your accounts. Users should never share their access information.
- Change your password every 30 days.** Avoid obvious passwords like your zip code, year of birth or personal information such as your mother's maiden name or your Social Security number. Symbols and/or upper and lower case letters make passwords harder to intercept.
- Update your anti-virus and anti-spam software.** This simple task makes it more difficult for scammers to access your confidential information and accounts. Anti-virus and anti-spyware software are available for purchase at major retail stores or on the Internet.
- Delete emails from unknown senders with questionable subject lines.
- When in doubt, call. Contact your National Penn Cash Management Support Area for assistance at 1.888.271.1666 if you have concerns that your accounts may be a target of fraud attempts. If you discover a breach of security, disable the user's ID immediately.

Our Commitment to Privacy

National Penn will never send unsolicited emails asking you to provide, update, or verify personal or account information such as passwords, EIN numbers, Social Security numbers, PINs, credit or check card numbers, or other confidential information.

Best Practices Checklist – Business e-Cash Manager

General

- Educate your employee users to **never** share passwords or divulge account or login credential information to anyone including fraudulent online email solicitations from the company's bank providers. National Penn has policies that prohibit the use of emails to request account or sensitive user ID information.
- Periodically throughout each day, review user activity reports available in most online cash management systems to ensure appropriate usage.
- Understand multifactor authentication controls offered by our Bank. Do not share answers to individual challenge questions with anyone.
- Ensure that all PCs in your company have current virus protection software and are protected by company firewalls.
- Rotate duties among employees **periodically**.

Online System Administration

- When employees leave **your organization** that **had** online user IDs, delete those IDs as part of your exit procedures.
- Remove online services and accounts from employee's user IDs that are not needed to fulfill their job function.
- Segregate duties and dual system administration responsibilities to allow for set up and verification of user ID maintenance tasks.
- Define transaction limits for all employee user IDs that initiate ACH and wire transfers.
- If not offered, request monthly password updates and use strong password formats (e.g. alphanumeric with length greater than 5 characters).
- When employees go on vacation, disable their computer access temporarily.

Payment Initiation

- Consider opening a separate, stand-alone account for outgoing ACH and wire transfer activity. Limit deposits to the account to the amount needed for outgoing ACH and wire transfers.
- Restrict individual user access at an account level.
- Do not include personal identification numbers such as Social Security numbers, in ACH addenda files.
- Segregate duties among employees for template maintenance, payment initiation and payment approval functions.
- Use bank-defined wire templates for high dollar, repetitive wire transactions.

This information was compiled by National Penn's Cash Management & Loss Prevention Departments. It is intended for educational and awareness purposes and may differ slightly from other related information. **These are strictly suggestions and practices that have been used by certain clients and us as potential ways to reduce the risk of fraud.** We encourage you to seek advice from qualified professionals.