Don’t Be Lured into a Phishing Scam

Don’t take the bait when criminals go “phishing” for your company’s assets.

“Phishing” is a scam in which criminals send deceptive emails in hopes of reeling in confidential or sensitive financial information that they can use to access and steal someone else’s money. Although the media have tended to spotlight individual victims, companies are often targets, too.

Phishing typically starts with an email that purports to be from a trusted source, such as a bank or government agency. The senders either suggest their email is simply a routine verification request, or inform you that your account will be closed immediately if you don’t provide the requested information. However, they’re aiming to trick you into disclosing information such as your firm’s bank account numbers, credit card numbers or PIN passwords. The thief uses this information to access your company’s accounts.

At U.S. Bank, we’re using the latest security methods to prevent this kind of fraud. But success requires our customers’ help. Here are some ways you can protect your business against criminals on phishing expeditions:

Never disclose sensitive information in an email. The single most important way you can protect yourself is to never disclose your company’s bank account, credit card account or PIN numbers by email. U.S. Bank and other legitimate companies will never request you to do so.

Always safeguard your company’s sensitive information. Change your ATM and Internet Banking account passwords regularly. If your password falls into the wrong hands, this will limit the damage that thieves can do.

Also, create passwords that are difficult to guess. For example, using a random combination of letters and numbers—something like j14Y33—is safer than using your name, birth date or other easy-to-remember combination. Use both upper- and lowercase letters if the passwords are case-sensitive.

Use different passwords for different purposes. That way a thief who steals one password can’t immediately access all of your accounts.

If you write down your passwords, don’t store them in your wallet or tape them to your computer. Don’t store them on your computer’s hard drive, either. Find a safe place that an unscrupulous person wouldn’t automatically search.

Finally, when discarding any papers that contain passwords or other sensitive information, shred them first.
Be suspicious of poorly written emails. Cyber-criminals are “spamming” large numbers of recipients—without actual knowledge of their banking affiliation—using fraudulent emails that include the logos and corporate look of widely known and respected financial institutions, including U.S. Bank. But sometimes scammers give themselves away with emails that are loaded with typos and grammatical errors.

Be suspicious of links to Web sites from emails. Sometimes a link from an email will take you to a page that mimics the look of your bank, when in fact the page is nothing more than a front for criminal activity. If you suspect a Web site is not what it claims to be, leave the site immediately.

Do not send sensitive personal or financial information unless it is encrypted on a secure Web site. Look for a padlock or an unbroken key symbol on the bottom bar of the browser to ensure that the site is running in secure mode before you enter sensitive information. Also look for an “s” after the usual “http” at the beginning of the Web address—“https://” indicates a secure, encrypted connection. Few criminals go to the effort of encrypting.

Report suspicious emails. If you’ve received a suspicious email, report it directly to your Internet Service Provider. If the sender claims to be U.S. Bank, please forward a copy to fraud_help@usbank.com along with your answers to the questions below:

- Do you have an account relationship with U.S. Bank?
- Have you recently enrolled for any U.S. Bank online services?
- What Internet Service Provider (ISP) do you use?
- What type of connection do you use to access the Internet? Cable, dial-up, DSL or other?
- Do you have a firewall installed on your computer?

If you have already received and replied to a suspicious email claiming to be from U.S. Bank, contact our Fraud Liaison Center immediately at 877-595-6256.