



Learn About Spoofs

Every Internet user should know about spoof (a.k.a. phishing or hoax) e-mails that appear to be from a well-known company but can put you at risk.

Although they can be difficult to spot, they generally ask you to click a link back to a spoof web site and provide, update or confirm sensitive personal information. To bait you, they may allude to an urgent or threatening condition concerning your account

What Spoof E-mails Are After

- Password or PIN
- Credit Card Validation (CCV) Code
- ATM/Debit or Credit Card number
- Social Security Number (SSN)
- Bank Account Number

Even if you don't provide what they ask for, simply clicking the link could subject you to background installations of key logging software or viruses.

Security Tip: NEVER click on a link contained in a suspicious e-mail.

Spot A Spoof

Although there's no foolproof formula for spotting a spoof e-mail or web site, these signs should arouse your suspicion:

Signs Of A Spoof E-mail

- There may be a **sense of urgency**. Example: Your account will be closed or temporarily suspended. You'll be charged a fee if you don't respond.
- There are **embedded** links that look legitimate because they contain all of part of a real company's name. These links may take you to spoof sites (or pop up windows) that ask you to enter, confirm, or update sensitive personal information.
- There may be obvious **spelling errors**. These help spoof e-mails avoid the spam filters that ISP's use.
- Spoof web sites can be more difficult to detect, because even the address bar and padlock that appear in your browser window can be faked. To make sure you're on a safe website, type in the root address (Ex. www.bloombank.com) to see if you get to the same place.

Protect Your Account

Educating yourself is the first step.

What You Can Do

- **Don't click on links in unsolicited e-mails**, especially those asking for personal information. Even if you don't supply it, just clicking can enable thieves to access your computer, record your keystrokes (key logging), and capture passwords you use to log on at various websites.
- **Go directly there.** The best way to get to any site is to type its address (URL) into your browser and then bookmark it.
- **Change Your Password and PINs Frequently.** Every 30-60 Days is recommended.
- **Keep Your Operating System and Browser Up-To-Date.** Software updates often include security enhancements that you can usually download free from www.netscape.com or www.microsoft.com, for example, Microsoft's site can even scan your computer and make sure that your software is up-to-date.
- **Check your account frequently.** With eBanking and EVE, our Touch Tone Teller, you can monitor you account transactions immediately without waiting for your monthly statement.
- **If you do not recognize a transaction or suspect fraudulent activity** on your account, call (800) 319-6110 immediately.

Other Security Tips

- **Create hard-to-guess passwords.** Use at least six characters and a mix of letters and numbers. Don't use all of part of your User ID or e-mail address, or the names of your children, spouse or pet. And use a different password for each of your online accounts.
- **Protect your identity.** Don't carry your Social Security card, Passport, or birth certificate – or those of your children – unless you need them that day.
- **Destroy all pre-approved credit offers that you don't respond to.**
- **Make sure your home computer has the most current anti-virus software.** Anti-virus software needs frequent updates to guard against new viruses. Make sure you download updates as soon as you're notified that they're available.
- **Install a personal firewall to help prevent unauthorized access to your home computer.** This is especially important if you connect to the Internet via a cable modem or a digital subscriber line (DSL) modem.
- **Stay Aware.** Visit bloombank.com/alert for information on scams and fraud attempts.

What we WILL NOT do

- We will **NOT** send urgent or time sensitive emails.
- We will **NOT** send emails asking you to provide, update, or confirm sensitive data.

- We will **NOT** send emails asking for personal information for your own security.
- We will **NOT** require you to enter anything other than your User ID and Password to sign on to our eServices.

Report A Spoof

If you suspect that you've received a fraudulent e-mail, please forward it to us immediately at: alert@bloombank.com

Note: Don't change or retype the subject line – this allows us to have the ability to properly investigate it. After forwarding the e-mail to us, you should delete it from your inbox.

You may also want to forward to the Federal Trade Commission (ftc.gov) at: Spam@uce.gov

Or contact them at:
consumer.gov/idtheft
1-877-IDTHEFT

Definitions

Spoof web site - spoof website is one that mimics a popular company's website to lure you into disclosing confidential information. To make spoof sites seem legitimate, thieves use the names, logos, graphics and even code of the real company's site.

They can even fake the URL that appears in the address field at the top of your browser window and the padlock that appears in the lower right corner. 🗝️ The links in the spoof e-mails almost always take you to a spoof web site.

Key Logging - This is another method used to capture your personal information. Here's how it works. You click on a link to a website or open an attachment that secretly installs software on your computer.

Once installed, it records everything you type, including any User IDs, Passwords and account or personal information. Thieves know how to retrieve this information, or even set it up to automatically have it sent back to them! This is a very real risk when using public or shared computers such as those in Internet cafes.