



Phishing, Vishing, Smishing – *Don't take the bait!*

Phishing

“Urgent! Your account has been suspended. Please visit this link to update your information and reinstate your account.” Have you ever received an email like this, from a company with whom you don't have an account? If so, you've been the target of a “phishing” scam.

The term “*Phishing*,” was intentionally coined as a play on “fishing.” Fishing is exactly what the scam artists are doing – throwing you deceptive bait to see if you'll bite and give up your personal information. Once they have that, scammers can make unauthorized charges to your bank account or credit card, or even open fraudulent accounts in your name.

Internet scammers are now well-known for sending mass emails (*spam*) or internet pop-up messages which seem to be from a friend or from a business or organization that you deal with – such as a bank, credit card company, or even a government agency. The message may ask you to “update,” “validate,” or “confirm” your account. Some phishing emails threaten serious consequences if you don't respond. The message will ask you to click on a link or call a phone number. It is very easy for con-artists to take logos or web images and recreate them to look and feel very legitimate or familiar. As real as the websites may seem, ***they are not legitimate.***

Malicious links

Don't click on any link in an email that may be phishy – scammers can display an impersonated organization's actual web address in a link while still sending you to a bogus site. Open a new browser and type in a web address you know to be correct, or call the organization using the phone number published in a directory. Since many consumers have started to catch on to the standard scams, fraudsters have had to employ more technologically sophisticated methods to phish for information. A link or attachment may lead to malicious software, known as “malware,” being installed onto your computer. Malware may allow a scammer to access your personal files, log your keystrokes to capture your passwords and account numbers, or even take control of your computer to send phishing emails to others.

Cyber imposters

Fraudsters may even use your identity to scam someone you know. If scammers are able to gain access to your email or social media accounts, they can contact your friends and family while posing as you. The scammers will change your password immediately upon accessing your account, thereby locking you out and cutting you off from all your contacts. They can then send urgent messages to all of your contacts, telling them that you've run into trouble, are stranded abroad and need money wired as soon as possible. By the time you are able to get the word out that you're okay, a well-intentioned friend or family member may have already wired money abroad. Also, many computer viruses are spread through compromised email contact lists. A familiar “from” address in an email is no guarantee of trustworthiness.

Spooftng

Spooftng commonly occurs when scammers use electronic devices to disguise their true identities or to hide the origins of their messages while phishing. In other words, the scammer will post a name or number on your email, phone caller ID, text message, or even internet URL as being from a person or place of business that you know and trust. Don't be fooled. The scammer behind the fake ID could be in another state or country using false names and titles that are impossible to trace.

Vishing & Smishing

After consumers started catching on to the phishing scams through email, scammers turned to a new method of targeting their victims by phone: **vishing**. Vishing is very similar to phishing, but scammers use telephone calls (either live or pre-recorded "robo-calls") instead of emails to try and lure people into giving up personal information. *Vishers* often rely on the use of posing as a local bank, credit union or other legitimate business that you might be inclined to trust or patronize. Since scammers can "spooft" any name and phone number that they want, the scammer can easily make a familiar or trusted business name appear on your caller ID. For example, a recorded message claims that the consumer's bank account has been compromised. When the consumer calls back, he/she speaks with a live person posing as a bank employee, who convinces the consumer that the only way to protect precious bank account information from criminals is to give the "bank employee" his/her personal information.

If you ever receive a vishing call from someone claiming to be an employee of your bank, credit card company, or any other business, call the actual business immediately to report the incident. Be sure to call using only a reliable telephone number obtained from your local phone book or from your paperwork with that business.

When the scam uses text messaging rather than a phone call or email, the scam technique is known as **smishing**. Typically, smishing text messages come from a "50000" number, instead of showing a typical phone number. This indicates that the message was sent from an email address, and not from an actual phone.

As with phishing and vishing scams, **you should not respond** to a smishing text message. If it seems to be a message from your bank or other business you're familiar with, contact that business using a reliable telephone number from your local phone book or from your paperwork with that business.

If you receive a phishing email, ask yourself:

- 1. Have I ever done business with this company?** If yes, still be cautious before clicking any links. If no, do not click any links and delete the email.
- 2. Are there any attachments with the email?** If yes, do not click on them. If you believe the email and attachment are legitimate, contact the sender first to verify the contents and security of the attachment.
- 3. Does the email request any personal information (such as social security number, Medicare card number, date of birth, credit card numbers, bank account numbers, or passwords)?** If so, do not reply. Delete the email.
- 4. Does the email contain grammatical errors and awkward sentences?** If so, do not reply. Many times phishers are from foreign countries. The grammatical errors are a red flag that the email is not from a professional, reputable and, most importantly, legitimate business.
- 5. Still not sure about the email's legitimacy?** If you still think that the email may be from a legitimate company that you have done business with (such as your bank or a government agency), look up a telephone number for that business or agency. Use a local, trusted phone directory or paperwork you have from the business (such as a bank statement or the back of a credit or debit card). Call the business or agency directly and ask them if they sent you the email.

What to do if you fall victim

If you believe you have fallen for a phishing, vishing or smishing scam, don't panic. There are simple measures you can take to monitor whether the scammers end up using your personal information to commit fraud.

- 1. Place a fraud alert on your credit report.** A fraud alert is a free service you can request from each of the three major credit reporting bureaus. The alert lets potential creditors know that you may be the victim of identity theft. A fraud alert can make it more difficult for someone to get credit in your name because it tells creditors to follow certain procedures in order to protect you. It stays on your report for 90 days (but can be renewed). You can request the fraud alert by calling each of the three major credit reporting bureaus:

Equifax (CSC Credit Services) 888-766-0008 www.equifax.com	Experian 888-397-3742 www.experian.com/fraud	TransUnion 800-680-7289 www.transunion.com
---	--	--
- 2. Check your free annual credit report regularly.** Obtain your credit report FREE from each of the three (3) major credit reporting agencies each year. Checking your report regularly is one of the best ways to protect against ID theft. We recommend you check one report once every four (4) months. You can get your free credit report from any of the three (3) – Equifax, Experian and TransUnion – by calling 1-877-322-8228, or online at www.annualcreditreport.com. Review your report for any inaccuracies or accounts you do not recognize. If you find errors or possible fraud, contact our office to find out what steps you can take to reverse the fraud or correct the errors.
- 3. Close out any financial accounts that may have been compromised.** If you gave out a credit card number or checking account number, call your financial institution and ask that the account be closed. Request that you be given new account numbers and card numbers. Ask your bank if you can place a password on your accounts. Some institutions may offer to monitor your account, but we highly recommend you completely close the compromised account. It's better to take the time now to follow the appropriate steps with your financial institution. Otherwise, you may need to spend time later to reverse hundreds or thousands of dollars in fraudulent charges.
- 4. If you gave out your driver's license number, contact the Division of Motor Vehicles.** Phone them at (608) 266-7425 or find them online at www.dot.state.wi.us.
- 5. To help reduce telemarketing calls, sign up for Wisconsin's No Call List.** Register your phone number (landline OR cell phone) by calling 1-866-9NO CALL (866-966-2255) or online at NoCall.Wisconsin.gov.
- 6. Contact our Office of Privacy Protection.** You can call 1-800-422-7128 or email us at DATCPWisconsinPrivacy@Wisconsin.gov. For more information, visit the website at www.privacy.wi.gov.

For more information and to learn more about how to minimize your risk of damage or to file a complaint, visit our website or contact the Bureau of Consumer Protection.

**Bureau of Consumer Protection
2811 Agriculture Drive
PO Box 8911
Madison WI 53708-8911**

E-MAIL: DATCPHotline@wisconsin.gov

WEBSITE: datcp.wisconsin.gov

Toll-free in WI: (800) 422-7128

TTY: (608) 224-5058

(608) 224-4976 FAX: (608) 224-4939