

Protecting Yourself from Online Scams

Since the Internet started growing explosively around two decades ago, email has provided individuals and businesses the enormous convenience of being able to communicate anytime and anywhere, wherever people can hook up to an Internet connection. With email, people can send messages with attachments such as photos, documents and other digital files. As more businesses welcomed email as an integral business communication tool, a lot of successful business transactions have been consummated solely through this marvelous electronic communication wonder.

However, the Internet, along with email as one of its components, has been created on the basis of trust. The early developers of the Internet exchanged ideas and collaborated freely on the early Internet as their platform for their research collaborations, trusting that they are communicating and exchanging classified files with people they know. But as the years progressed, and as email and the Internet advanced as a whole, the number of users exchanging messages through the Internet has grown tremendously.

Today, many perpetrators of online theft are devising schemes that are aimed at grabbing unsuspecting individuals' personal data. Some online thieves are even creating means to penetrate businesses and take away precious corporate information. One such scheme is [phishing](#). Phishing is a fraudulent online correspondence that has been created to dupe people into giving away personal information such as credit card numbers, TIN numbers, bank account numbers and ATM card PINs. Phishing can also



take your Web identity, allowing the perpetrator to transact business online using your identity and other information that is pertinent to you.

Hackers who carry out phishing campaigns do so by sending emails that usually ask you to confirm or update information including your bank account number, your email password and ATM PIN number. One such phishing scam is an email disguised as coming from a bank. Other scams are posed as messages coming from online payment services such as [PayPal](#) or Xoom, asking you to validate your username and password.

It is sad to note that thousands of people and many businesses have already been deceived, and have lost millions of dollars in the process. And as more and more people and corporate entities have become aware of this fraudulent activity, online scammers have been diligently working on other schemes that they believe they can pull off to steal other people's hard-earned money.

To avoid having you or your business become a victim to phishing and other online scams, here are some practical tips from [ThinkPlanInvest.com](#).

10 Steps to Avoid Falling Prey to Phishing Scams

1. If you are doubtful about the credibility of the email, DO NOT click on any link provided in the email. This may trigger malicious codes to be installed on your PC.



2. Before you share any information on a website in response to an email, always ensure that the URL shown in the email matches the URL of the bank website. If it does not, you have valid reason to suspect that there's something fishy.
3. Do not open unexpected e-mail attachments or instant message download links.
4. Check the web address carefully. One trick is to mouse over the link that has been sent to you. The actual destination URL is shown on the bottom of your browser. If it is not the website you thought or if it has strange extensions, like ".cn" or any other foreign country extension do not click on it.
5. Check for the Padlock icon at the bottom right corner of the webpage. It must be always 'On' during secure transactions.
6. Ensure that you have installed the latest anti-virus/anti-spyware/personal firewall/security patches on your computer.
7. Always use a non-admin user ID for daily work on your computer.
8. Do not access banks or make payments using your debit or credit card from shared or unprotected computers in public places like cyber cafes.
9. Do not transfer funds to or share your account details with unknown/non-validated sources, especially those luring you with commissions, attractive offers or prizes.
10. If you receive an email from a friend and the tone or language is out of character, don't open any attachments or follow any links. On Facebook a common phishing scam



has included getting messages from friends with links that install a Trojan horse if you follow the link. The links come from hacked accounts.

To find help in securing your IT system, visit [All Covered](#) or call 866-446-1133.

Contact All Covered Toll-Free Nationwide at (866) 446-1133 or at www.allcovered.com

©2009 All Covered, Inc. All rights reserved. All Covered is a registered trademark of All Covered, Inc.