Protect Yourself from Phishing

There is only one of you and we prefer to keep it that way. That’s why we believe it is important to educate you on the various ways you can protect yourself from the risk of identity theft.

What is Phishing?

Phishing emails are crafted to look as if they’ve been sent from a legitimate organization. These emails attempt to fool you into visiting a bogus web site to either download malware (viruses and other software intended to compromise your computer) or reveal sensitive personal information. The perpetrators of phishing scams carefully craft the bogus web site to look like the real thing. Bogus communications purporting to be from banks, credit card companies, and other financial institutions have been widely employed in phishing scams, as have emails from online auction and retail services. Carefully examine any email from Reliant Bank and other financial institutions. Most have instituted policies against asking for personal or account information in emails, so you should regard any email making such a request with extreme skepticism.

Phishing emails have been disguised in a number of ways. Some of the most common phishing emails include the following:

• Fake communications from online payment and auction services, or from internet service providers – These emails claim there is a “problem” with your account and request that you access a (bogus) web page to provide personal and account information.
• Fake accusation of violating Patriot Act – This email purports to be from the Federal Deposit Insurance Corporation (FDIC). It says that the FDIC is refusing to ensure your account because of “suspected violations of the USA Patriot Act.” It requests you provide information through an online form to “verify your iden
tity.” It’s really an attempt to steal your identity.

How do you avoid being a victim?

Be suspicious of any email with urgent requests for personal financial information.

• Phishers typically include upsetting or exciting (but false) statements in their emails to get people to react immediately.
• They typically ask for information such as usernames, passwords, credit card numbers, social security numbers, date of birth, etc.
• Phisher emails are typically NOT personalized, but they can be. Valid messages from your bank or e-commerce company generally are personalized, but always call to check if you are unsure.

Don’t use the links in an email, instant message, or chat to get to any web page if you suspect the message might not be authentic or you don’t know the sender or user’s handle.

• Instead, call the company on the telephone, or log onto the website directly by typing in the Web address in your browser.

Avoid filling out forms in email messages that ask for personal financial information.

• You should only communicate information such as credit card numbers or account information via a secure website or the telephone.
Always ensure that you're using a secure website when submitting credit card or other sensitive information via your Web browser.

- Phishers are now able to 'spoof,' or forge BOTH the "https://" that you normally see when you're on a secure Web server AND a legitimate-looking address. You may even see both in the link of a scam email. Again, make it a habit to enter the address of any banking, shopping, auction, or financial transaction website yourself and not depend on displayed links.
- Phishers may also forge the yellow lock you would normally see near the bottom of your screen on a secure site. The lock has usually been considered as another indicator that you are on a 'safe' site. The lock, when double-clicked, displays the security certificate for the site. If you get any warnings displayed that the address of the site you have displayed does NOT match the certificate, do not continue.

Regularly log into your online accounts and regularly check your bank and credit card statements to ensure that all transactions are legitimate.

- If anything is suspicious or you don't recognize the transaction, contact your bank and all card issuers.

You can report "phishing" or “spoofed” e-mails to the following groups:

- Forward the email to the Anti-Phishing Work Group at reportphishing@antiphishing.org and/or the Federal Trade Commission at spam@uce.gov.
- File a complaint through the FTC at www.ftc.gov.
- When forwarding spoofed messages, always include the entire original email with its original header information intact.

**What do you do if you think you are a victim?**

If you believe your financial accounts may be compromised, contact your financial institution immediately and close any accounts that may have been compromised. Watch for any unexplainable charges to your account.

Immediately change any passwords you might have revealed. If you used the same password for multiple resources, make sure to change it for each account, and do not use that password in the future.

Consider reporting the attack to the police, and file a report with the Federal Trade Commission (http://www.ftc.gov/).

Many email scams have existed for a long time. In fact, a number of them are merely “recycled” scams that predate the use of email. The FTC has a list of the 12 most common scams (http://www.ftc.gov/opa/1998/07/dozen.shtm). The list includes:

**Bogus business opportunities & work-at-home schemes**
- These scams promise the opportunity to make a great deal of money with very little effort. They’re normally full of enticements such as “Work only hours a week,” “Be your own boss,” “Set your own hours,” and “Work from home.”

**Health and diet scams**
- These scams attempt to lure consumers with promises of quick fixes and amazing results, discount pricing, fast delivery, waived prescription requirements, privacy, and discreet packaging.

**Chain letters**
**Easy money**
**“Free” goods**
**Investment opportunities**
Bulk email schemes
Cable descrambler kits
“Guaranteed” loans or credit

Remember that even email sent from a familiar address may create problems: Many viruses spread themselves by scanning the victim computer for email addresses and sending themselves to these addresses in the guise of an email from the owner of the infected computer.