



Quick Fact:

*1 in 4 Americans risk being a victim of identity theft.**

National Consumer Protection Week

Tip Of The Day

Phishing, Vishing & Smishing: ID Theft Scams

Phishing

- Internet identity thieves send bogus e-mails claiming to be legitimate companies, organizations and even government agencies like the IRS to get Web users to provide personal information like credit card and social security numbers, passwords or other sensitive information.
- Phishing e-mails instruct recipients to click on a link in the e-mail to open a page that appears nearly identical to a Web page for a well known retailer, bank or other business. The link actually connects to a bogus site that will capture any personal or financial information entered.

Vishing (Voice Phishing)

- Vishing thieves send bogus e-mails that tell users to call a number rather than clicking on a link. When the victim calls the number, they will hear an automated answering service asking for account information. Once provided, the victim becomes vulnerable to identity theft.
- Vishing scams recently included emails written to appear as if they came from PayPal indicating a problem with the recipients' account.
- Vishing scams mimic the legitimate ways people interact with financial institutions.
- Some victims of vishing receive calls from suspects that already have the recipient's credit card number and ask just for the three-or four-digit security code on the back of it.
- Voice Over Internet Protocol (VoIP) technology enables cheap and anonymous Internet calling and can trick caller ID boxes into displaying fraudulent information.

Smishing

- Smishing scams are delivered via text messages over cell phones and other devices.
- Bogus text messages are sent to recipients asking for personal information and threatens exorbitant fees unless they respond and contact the sender.
- Some smishing scams attempt to download Malware onto your phone by offering "great deals" on products.

Warnings

- Do not respond to unsolicited text messages.
- Legitimate companies, organizations or government agencies won't contact you unexpectedly asking for your personal information.
- Don't click on emails asking for personal information. Such emails could lead to fake versions of legitimate Web sites to obtain your personal information.
- Never enter personal information on pop-up screens that may be planted on legitimate Web sites.
- Use a spam filter, up-to-date anti-virus, anti-spyware software and strong firewalls to keep malicious messages and programs from phishers off your computer.
- Beware of "pharming" con artists that plant programs in your computer to hijack your browser and go to phishing sites.

*Federal Trade Commission

Be an educated consumer!

**Visit www.hillsboroughcounty.org/consumerprotection
Hillsborough County Consumer Protection Agency | 813-903-3430**