



## TampaNewsAndTalk.com

**Nancy L. Janssen**  
Columnist

### Staying Safe on the Internet

How could we live without the Internet? That's how most of us keep in touch with friends, find homework support, and research a cool place to visit, or find out the latest news.

There are steps you can take to staying safe on the Internet. The key is to protect yourself while online, remain as anonymous as possible. That means keeping all information private. Never give out your full name, home address, phone number, Social Security number, Passwords, names of family members or credit card numbers. People you meet online can claim and say anything whether it's true or not.

Everyone is at risk whether they know it or not. Never use a screen name as a password and change your passwords frequently. No matter what age you are you and your computer are vulnerable to hackers, scammers and criminals.

Getting Suspicious Emails? Want to know the source of suspicious emails?

[http://www.ip-adress.com/trace\\_email/](http://www.ip-adress.com/trace_email/)

Filter Tips:

Top 10 Scams to Screen from Your Email

- The "Nigerian" Email Scam
- Phishing
- Work-at-Home Scams
- Weight Loss Claims
- Foreign Lotteries
- Cure-All Products
- Check Overpayment Scams
- Pay-in-Advance Credit Offers
- Debt Relief
- Investment Schemes

This site pretty much says it all  
<http://www.onguardonline.gov/topics/overview.aspx>

Phishing is a scam where internet fraudsters send spam or pop-up messages to lure personal and financial information from unsuspecting victims. To avoid getting hooked don't reply to any email or popup message that asks for personal or financial information and never click on links in any message. Do not cut and paste a link from the message in your web browser----phishers can make links look like they go one place, but that actually send you to a different site.

Some scammers send an email that appears to be from a legitimate business and ask you to call a phone number to update your account or access a "refund." Because they use Voice over Internet Protocol Technology, the area code you call does not reflect where the scammers really are.

If you need to reach an organization you do business with, call the number on your financial statements or on the back of your card.

1. Don't email personal or financial information.
2. Review credit card and bank account statements as soon as you receive them to check for unauthorized charges.

Be cautious about opening any attachment or downloading any files from emails you receives regardless of who sent them.

Forward phishing emails to [spam@uce.gov](mailto:spam@uce.gov) - and to the company, bank, or organization impersonated in the phishing email. You also may report phishing email to [reportphishing@antiphishing.org](mailto:reportphishing@antiphishing.org). The Anti-

Phishing Working Group, a consortium of ISPs, security vendors, financial institutions and law enforcement agencies, uses these reports to fight phishing.

If you've been scammed, visit the Federal Trade Commission's Identity Theft website at [ftc.gov/idtheft](http://ftc.gov/idtheft).

How Not To Get Hooked by a "Phishing" Scam.

"We suspect an unauthorized transaction on your account. To ensure that your account is no compromised, please click the link below and confirm your identity."

"During our regular verification of accounts, we couldn't verify your information. Please click here to update and verify your information."

Have you received email with a similar message? It's a scam called "phishing" – and it involves internet fraudsters who send spam or pop-up messages to lure personal information (credit card numbers, bank account information, Social Security number, passwords, or other sensitive information) from unsuspecting victims.

According to OnGuard Online, phishers send an email or pop-up message that claims to be from a business or organization that you may deal with – for example, an Internet Service Provider (ISP), bank, online payment service, or even a government agency. The message may ask you to "update," "validate," or "confirm" your account information. Some phishing emails threaten a dire consequence if you don't respond.

The messages direct you to a website that looks just like a legitimate organization's site. But it isn't. It's a bogus site whose sole purpose is to trick you into divulging your personal information so the operators can steal your identity and run up bills or commit crimes in your name.

Use anti-virus and anti-spyware software, as well as a firewall, and update them all regularly. Some phishing emails contain software that can harm your computer or track your activities on the internet without your knowledge.

If you don't recognize the sender and in the subject line it says "No Subject" Delete it, it's not worth being curious.

If you've received spam that is phishing for information:

Forward it to [spam@uce.gov](mailto:spam@uce.gov) – and to the company, bank, or organization impersonated in the phishing email. Most organizations have information on their websites about where to report problems.

If you believe you've been scammed:

File a report with the Federal Trade Commission at [www.ftc.gov/complaint](http://www.ftc.gov/complaint)

Report it to your state Attorney General, using contact information at [naag.org](http://naag.org).

Then visit the FTC's identity theft website at [ftc.gov/idtheft](http://ftc.gov/idtheft). While you can't completely control whether you will become a victim of identity theft, you can take some steps to minimize your risk.

There are many good software programs. I use CNET as my source for trusted programs such as Advanced System Care and Ccleaner also Avast

and Avg. These are free programs to help keep your computer clean and free of viruses.

Make sure you select the free ones and not the ones that cost\$.

**Breakfast**  
Served with coffee or tea

From **\$6.99** (M-F) subtract discount



**\$2 Off** Lunch & Dinner  
W/ coupon\* **\$1 off Breakfast**

**5299 E. Busch Blvd, Tampa**  
1 Mile East of Busch Gardens/ near 56 Street

Have fun at Busch Gardens & then come eat at Lupton's !!

Open 7 days per week from 7 A.M. To 9 P.M.

**TampaNewsAndTalk.com**

\* Valid for 1 (one) meal, per person, per day, 7AM & 9PM, Mon-Fri. This offer can not be used with any other offer special or discount promotion. Offer expires 10-1-2011.

**TampaNewsAndTalk.com**



**News & Editorials**  
Investigative Reporting  
Community Talk Shows  
Public Relations

**Al Mccray**  
Managing Editor  
813.244.0664

P.O. Box 280486, Tampa, FL 33682

**FREE** 20 oz. Drink

With purchase of Any Footlong Subway Sandwich  
Must present coupon.  
Not valid with any other offers.  
**LIMITED TIME OFFER**



**PEPSI** 12 PACKS  
**2 for \$7.00** +TAX  
**ALL PEPSI PRODUCTS**

Must present coupon. Not valid with any other offers.  
**LIMITED TIME OFFER**

**Radiant Food Stores**

Sandwiches  
Groceries • Beer/Wine  
Beverages • Cigarettes  
Gas • Car Wash

**SUBWAY**

**ONE STOP DOES IT!**

1521 W. Fletcher Avenue • Tampa  
**813-264-0551**  
(Located N.E. corner of Fletcher at Rome)



VISA, MasterCard, Discover, American Express, Florida Lottery

