Surf Safe & Secure

Some easy tips to help keep your online experience safe:

- **Install and consistently update** anti-virus, anti-spam and security software, taking time to ensure you aren't using unsupported software.
- **Beware of downloading free software** or software from an unfamiliar source. It could be bundled with spyware or other programs harmful to your computer.
- If you don't know the source of an email, don't open it. Delete it.
- To avoid identity theft and protect your privacy, **choose a password made of random numbers and letters and memorize it.** Passwords such as your father's first name and digits of your Social Security number can sometimes be determined by hackers.
- Only share credit card and other personal information when you're buying from an established company you trust.
- **Do NOT answer pop-up messages** or emails that ask you to update your account information. Legitimate requests will ask you to visit your protected online account.
- Do NOT cut and paste into your browser a web address that is located in the body of a suspicious or unfamiliar email. The perpetrators will make an illegitimate address look very similar to the legitimate one.
- Never pay for a "free" gift.
- On social networking sites, **don't choose a screen name that gives too much of your identity away.**
- If using a public computer, do NOT save log-in information, such as passwords or screen names. **Be sure to log off a website before leaving the computer.** Even better, close the browser.

For more information visit: www.att.com/safety

at&t

Familiarizing yourself with these online terms will help keep you surfing safely:

Phishing: Claiming to be a legitimate business in an attempt to scam user into providing private information that will be used for identify theft. Some examples include bank, credit card and email passcodes.

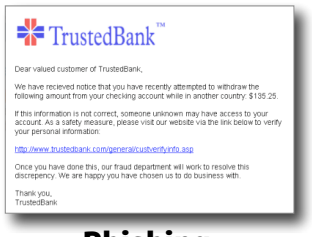
Pop Ups: Online advertising that opens in a new window or tab to attract web traffic or capture email addresses.

Spyware: Software installed on your computer without your knowledge that takes over partial control of your computer or collects information on your computer.

Spam: Sending unsolicited bulk email messages.

Computer Viruses: Computer programs designed to gather information, destroy data, disrupt usage and are installed without the user's knowledge.

SOME EXAMPLES INCLUDE:



Phishing

Spyware

Pop Ups

Spam

Stay Vigilant About Identity Theft:

Possible Signs you are a Victim:

- Negative notations on your credit report
- You don't receive regular bills
- Receiving credit cards you did not request
- Loan denial
- Phone calls or collection letters from unknown creditors
- Bills for merchandise you did not order or accept

Resources if you have been a Victim:

- Local Police
- Federal Trade Commission 1-877-IDTHEFT
- Credit Bureaus:
  - Experian: 1-888-397-3742
  - Equifax: 1-800-525-6285
  - TransUnion: 1-800-680-7289
- Your bank
- Better Business Bureau (www.bbb.org)
- State Attorney General

For more information visit: www.att.com/safety

at&t