FRAUD ALERT BULLETIN

As part of our ongoing efforts to help keep your personal information safe, we want to remind you to stay on the lookout for the many e-mail scams making the rounds in cyberspace today.

We've recently been notified of fraudulent e-mails claiming to come from the following companies: UPS, Domain Names, Newegg.com, USPS, Wells Fargo, PayPal, Chase Bank, Verizon Wireless, the SEC, PayFlow, Intuit, the IRS, Amazon, and FedEx. **In all of these fraud attempts, the messages request that recipients provide some type of personal information.**

If you receive any of these e-mails

- **First, delete the e-mail immediately and don't click on any link or open any attachment**—it could install malicious software (malware) that could potentially access all username and password information stored on your computer.
- In addition, keep in mind that **no legitimate organization requests personal data or information via e-mail**. If a message requests this type of information from you, consider it a major red flag.

How to protect yourself

Keep the following tips in mind to protect yourself from cybercriminals:

1. As noted above, **don't click on any links or attachments** within suspicious e-mails or text messages. Sign in directly to the company's website to check messages and perform other actions.
2. **Be wary of links from people you don't know** or of messages that don't read the way a friend would normally write.
3. **If you accidentally access a dangerous attachment** and believe a password-stealer is running on your computer, **contact a technology specialist as soon as possible.**
4. **All unsolicited e-mails concerning password or account changes**—especially those that contain attachments—**should be considered scams until verified.** Log in to the account in question to check the situation.
5. **Do not respond to text messages or automated voice messages from unknown or blocked numbers** on your mobile phone.
6. **Use a credit card when purchasing online.** Charges can be disputed if you don't receive what you order or if you discover unauthorized charges on your card.
7. **Check the seller's ratings and feedback, as well as the dates they were posted.** Be wary of a seller with a 100-percent positive feedback score, a low number of feedback postings, or with all feedback posted around the same time.
8. **Never respond to suspicious, unsolicited e-mails, texts, phone calls, or voicemails that request personal information.** If you are unsure of the validity of the message or call, go to the company's website directly.

Rest assured that helping you keep your personal information safe is one of our top priorities. If you have any questions about the material presented here, please contact us at (408) 286-8483.