

Email Tips to Avoid 'Phishers' & Scams

You can never be too careful when it comes to protecting your personal information. Here are some other things to watch for:

1. **Is the email addressed to you personally?** Many phishers send fake emails that use generic greetings, such as "Dear Customer" or "Dear Sir/Madam." Official emails are personalized with the name you gave us when you registered.
2. **Does the email read well?** Fake emails are often littered with misspellings, poor grammar, etc. These mistakes actually help them avoid spam filters, but they should be a dead give-away that they are not from the real site. Business emails are written with care and proofread by professionals.
3. **Does the email ask you for information?** If you get an email or pop-up message that asks for personal or financial information, do not reply or click on the link in the message. Legitimate companies don't ask for this information via email. Beware of any email that asks you to provide:
 - a. Credit or debit card numbers
 - b. Driver's License numbers
 - c. Passwords
 - d. Bank account numbers
 - e. Social Security numbers
 - f. Your full name
 - g. Birthdate
 - h. Email addresses
4. **Where does the link take you?** The links in fake emails rarely show you the actual web address - they'll usually hide the address within a phrase like "Click here" or "Log in."
5. **Is the web page secure?** Any time you're asked to give personal information on a web page, the web address should begin with "https:". The "s" stands for "secure" and is your key to knowing your information is protected.
6. **Never email personal or financial information.** Email is not a secure method of transmitting such information.
7. **Review credit card and bank account statements** as soon as you receive them to determine whether any unauthorized charges appear.
8. **Use anti-virus software and keep it up to date.** Some phishing emails contain software that can harm your computer or track your activities on the Internet without your knowledge.
9. **Be cautious about opening any attachment** or downloading any files from emails you receive, regardless of who appears to have sent them.
10. **Report suspicious activity to the FTC.** If you believe you've been scammed, file your complaint at <http://www.ftc.gov/>.