Identity thieves use fraudulent email scams, or "phishing" scams, to trick you into giving away your vital personal information such as usernames, passwords, credit card details and other account information. Phishing is typically carried out by email, and it often directs users to enter details at a fake website designed to look almost identical to the legitimate one. Follow these steps to protect yourself from phishing scams:

1. Determine if the nature of the correspondence is suspicious.

- Phishing correspondence will usually ask you for sensitive, personal information that the organization should already have. For example, if your bank sends you an email asking you to provide them with your account number, it may be a phishing scam.
- In some cases, phishing correspondence may be written to induce panic or assume a threatening tone designed to make you act immediately.

2. Review suspicious emails and text messages for spelling and punctuation.

- If the email or text message is coming from a major business or corporation, it is unlikely that spelling and punctuation errors will be published.

3. Call the organization directly to verify the inquiry.

- Mention to the organization that you received suspicious correspondence and you need to verify its authenticity.
- If you were left with a voice mail or automated message providing you with a phone number to call, verify that the phone number matches with the phone number for that organization.

4. Examine the website links and logos in suspicious emails you receive.

- Hover your cursor over the link or business logo within your email. A small pop-up bar that displays the true website address will appear below the link embedded within the email.
- Refrain from clicking or visiting any unfamiliar links that end with a .exe extension. Exe. links may cause you to download malicious software, spyware, or other programs that can steal your personal information.

5. Examine the email address of the entity that sent you the email.

- Sometimes, phishing scams will display email addresses that resemble authentic company email addresses, but vary slightly enough to trick you.

6. Provide your personal information only to websites that are secure.

- Look at the address bar of the website you are visiting to determine if the site begins with https rather than http. The https part of the web address indicates the website is secure.
- A yellow padlock icon displayed toward the bottom of your web session can also help you determine a website's security. Double-click on the padlock icon to verify that a security certificate displays on the screen, as some websites will display just a graphic of a padlock to be malicious.

7. Review your bank statements regularly.

- If you notice any unauthorized activity in you bank account or on credit cards, notify your financial organizations immediately. This may prevent the cyber criminals behind the phishing scam from continuing to use your information.

POLAR

Source: http://www.wikihow.com/Protect-Yourself-from-Phishing-Scams