

Phishing (pronounced as fishing)

In the field of computer security, phishing is the criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication.

Communications purporting to be from popular social web sites, auction sites, online payment processors or IT administrators are commonly used to lure the unsuspecting public.

Phishing is typically carried out by e-mail or instant messaging,<sup>[1]</sup> and it often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one.

Phishing is an example of social engineering techniques used to fool users,<sup>[2]</sup> and exploits the poor usability of current web security technologies.<sup>[3]</sup>

Attempts to deal with the growing number of reported phishing incidents include legislation, user training, public awareness, and technical security measures.

The best way to protect yourself if you are unsure is to go type the address of the web site into the address bar directly so that you know you are going to the official website. Then sign on if that is what you need to do and verify that your information is secure.

Never connect to a link from an email that looks like it came from your bank, credit card company or other services that have your sensitive information.

Just delete the phishing email –never respond!