

What is Phishing?

The latest Identity Theft scam to hit the Internet is called Phishing, which is pronounced like fishing. This scam sends users a simple e-mail that looks like it came from an Internet Service Provider (ISP) or eBay, Best Buy or any other major company. The e-mail states there is a problem with your account or it advises you of a "Fraud Alert".

The e-mail will say that in order to correct the problem they need you click on the link in the e-mail. The link will take you to a web site that asks you to provide information such as Social Security and credit card numbers. This web site is a fake. If you fill in the information, you are giving your personal information to people that are going use it for "no good".

You should be wary of any e-mail that you receive that asks you to provide information such as Social Security Number, Credit Card Number or Passwords. As a side note RUCS-Newark will never ask you for your Security Number, Credit Card Number or Passwords via e-mail.

There are a few simple things you can do to help protect yourself from Identity Theft:

- Don't fill in personal information via a link in and e-mail.
An e-mail link can be faked. You should always go to the company's main web site. If it is truly a serious problem, the web site will have information posted on the main page of the web site.
- Always check your credit card statements for strange transactions or transactions you don't recall.

Identity Theft is one of the fastest growing crimes, don't become one of the statistics.

For more information on Identity Theft visit either of these two sites:

<http://www.consumer.gov/idtheft/> or

<http://www.idtheftcenter.org>