



ONLINE SAFETY TIPS

“PHISHING”

WHAT IS PHISHING?

Phishing is an online scam used to commit identity theft. A fraudulent, but official-looking e-mail is sent to a user in an attempt to con that user into divulging personal and/or private information, which is then used for identity theft.

HOW IT WORKS

Phishers spam huge numbers of users with a seemingly credible e-mail that instructs the user to visit a Web site (also fraudulent) where they are prompted to enter or update their personal or private information (such as passwords and credit card, social security, and bank account numbers). Phishers also use pop-ups to try and scam users into entering sensitive information. What actually happens, to the trusting users who submit this information in response to a Phishing attempt, is that identity thieves steal the user's information and their accounts are emptied.

HOW TO PROTECT YOURSELF

- Do not reply to any e-mail asking to verify your personal data. You will find that legitimate vendors and merchants do not send such requests via e-mail.
- Contact your merchant right away to ask for clarification of such e-mails. (This will also make them more aware of the range of such problems.)
- Never divulge information, such as passwords and credit card, social security, and bank account numbers, to anyone making contact with you. Only give such information when you initiate a service call, and only do so with trusted sources and where appropriate.
- Use anti-virus software and/or firewalls on every computer you own/use. Remember that children are easy prey to the 'just click here' tactic.

**For more information, contact the Binghamton Police Department's
Crime Prevention Unit at (607) 772-7093**