SECURITY TIPS

Phishing

May 2012

Phishing - How to Avoid Getting Hooked!

What is Phishing?

Phishing is a scam which attempts to entice email recipients into clicking a link that takes them to a bogus website. The website may prompt the recipient to provide personal information such as social security/TRN number, bank account or credit card number, and/or may download malicious software onto the recipient's computer.

How do I know it is a Phishing Scam?

- If you receive an email appearing to be from a legitimate business, requesting you submit personal information, it is most likely a scam. Legitimate businesses DO NOT send emails requesting personal information.
- If you have received a suspected phishing email, please notify LIVE@jnbs.com

What Can I Do?

- Think before you click.
- Do not click on any links listed in the email message and do not open any attachments contained in suspicious email.
- Do not enter personal information in a pop-up screen. Legitimate companies, agencies and organizations don't ask for personal information via pop-up screens.
- Ensure that your computer and antivirus program is installed and up-to-date.
- Use bookmarks in your web browser for the organizations with which you regularly communicate, to limit the chances of being redirected to malicious sites.
- Look for unauthorized charges or withdrawals on your credit card and bank statements/bills.
- Do not respond to unsolicited (spam) incoming e-mails.
- Beware of emails that reference any consequences should you not "verify your information".

