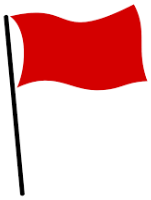
E-Mail Security Red Flags



Cyber-attacks are growing in number each year and becoming increasingly dangerous to businesses. Many recent cyber-attacks have been a result of social engineering via e-mail. Attackers can now gather just enough personal information to make an e-mail very convincing. With proper filters in place, most spam e-mails are stopped before reaching any users, however, the threat is always there.

The following seven red flags may indicate that an e-mail is not to be trusted:

1. You receive an e-mail requiring immediate action or it creates a sense of urgency – this is a common method used to trick people into doing things before thinking it through.

2. The message contains "Dear Customer" or other generic salutation.

3. The message has poor grammar and spelling – most businesses proofread their messages.

4. The message has a suspicious link. You can see the true destination of a link by "hovering" your mouse over it. In spam e-mails the destination URL may be different from the link written in the e-mail. Cyber criminals are getting more sophisticated so the URL may appear to be valid. **When in doubt, don't open any links and get confirmation from your IT Department or contact the sender directly.**

5. Hyperlinks that are embedded in an e-mail are often used for phishing. **Do not open the link and check with your IT Department.**

6. Receiving unexpected documents – **Only open attachments that are from sources you know and are expecting.**

7. Do not open messages that seem odd or make you suspicious. Double check the e-mail address that the message is coming from and ensure it is valid. **When in doubt, delete and contact the sender separately through phone.**

Please share this information with employees to minimize the chances of an attack happening to you.

Business Services Group | National Exchange Bank & Trust
1-877-495-6989 | businessbanking@nebat.com | www.nebat.com