GOOD PRACTICES: Emails/Communications for Service Consumers

1. Beware of messages with typos, grammatical errors, or which appear to imitate a known source; for example, a message from someone representing themselves as university personnel using an address other than @unh.edu.

2. Be careful of messages that do not look like the customary communication from the sender; if the format, writing style or even the colors seem different than the usual, it may indicate a malicious message.

3. Watch for instructions or requests in the message that put you at risk; for example, asking for your password or credit card number for any reason.

4. When including links reference only well-known top level URLs that the reader can verify as being legitimate, such as www.unh.edu. Avoid links that are visually complicated and minimize sending clickable links. Urge the reader to avoid clicking on the URL; rather, instruct the reader to type the URL into their browser.

5. Do not open attachments in email messages unless you are confident that they are safe. Even well meaning friends may unknowingly send you an attachment that is infected or otherwise malicious. Scan any attachment with up-to-date antivirus software before opening.

6. Check with the sender through another form of communication, such as by telephone, if you are not sure that the message came from the sender.

7. Look for indications that the sender is choosing safe communication methods, such as standard university websites or newsletters, and/or explains how they are protecting you.

See http://www.onguardonline.gov/ and http://www.scamdex.com/ for more information on protecting yourself.

GOOD PRACTICES: Emails/Communications for Service Providers

1. Create email messages that are short, to the point, for a specific purpose, and from a verifiable sender; include only what your email readers need to know or do.

2. Offer clearing house/reference contact info, such as your university phone number, so that recipients can verify the email.

3. For departmental emails, maintain a visual identity that is difficult to replicate and aggressively protect that identity.

4. When including links, reference a well-known top level URL such as unh.edu, avoiding links that are visually complicated; minimize the use of clickable links.

5. Do not add attachments for volume e-mails; put the information in the body of the email or on a trusted website and direct your readers to that website.

6. Use the BCC field rather than the CC or TO field for volume mailings to protect the privacy of those receiving the communication. This is not necessary when sending email to working groups and other coherent organizations.

7. Use Blackboard for protected communication to students.

8. Use a website and/or other standard university communication, such as UNH Today, for detail information and refer your readers to that communication.

9. Explain how your method of delivery is for the recipient's protection.

See http://www.onguardonline.gov/ and http://www.scamdex.com/ for more info on how to provide protection to communications recipients.

IT Security, 4/26/2010