Beware of Holiday Season Fraudsters

The holiday season provides increased opportunities for malicious actors to conduct seasonal phishing and malware campaigns as a means to gain unauthorized access to computer systems. Over the course of the holiday season, please continue to practice safe browsing and to evaluate e-mails, text messages, and other communications with a critical eye.

Please be aware that cyber actors may leverage the sales, good will, and other aspects of the holiday season to entice individuals into opening attachments, clicking links, or installing software that contains malicious code or collects personal information. Customers should practice safe internet browsing both on personal and corporate computer systems.

Potential attack vectors include:

- Seasonal E-Cards/E-mails
- E-mails/In-mails on social networking sites
- Fraudulent posts on social networking sites
- Fake advertisements
- Fake shipping notifications, with attachments or links to view the notice
- Charity scams

Protective measures against phishing scams and malware campaigns include:

- Maintain up-to-date antivirus software
- Maintain up-to-date, patched software
  (operating systems, internet browsers, Adobe Flash, Silverlight, etc...)
- Do not follow unsolicited web links in email, text, or chat messages
- Use ad-blocking software to avoid 'malvertising' and downloading of malicious content
- Do not open unexpected attachments
- Save and virus scan attachments before opening them
- Do not provide personal or corporate information over the phone, through a website, or via email to unknown persons or to an unsecure web site.
- Verify the identity of the person with whom you are communicating