White and Williams LLP

Department of Homeland Security Issues Internet Security Alert Ahead of Easter Holiday

By: Linda Perkins
Cyber Law and Data Protection Alert
4.13.17

On April 11, 2017, the United States Computer Emergency Readiness Team (US-CERT) for the U.S. Department of Homeland Security issued an alert through its National Cyber Awareness System reminding internet users to stay aware of Easter holiday phishing scams and malware campaigns. These releases are intended to inform the public and business owners of suspected online threats.

In particular, US-CERT has identified a need for increased vigilance concerning:

- unsolicited shipping notifications that may actually be scams by attackers to solicit personal information (phishing scams),
- electronic greeting cards that may contain malicious software (malware),
- requests for charitable contributions that may be phishing scams or solicitations from sources that are not real charities, and
- false advertisements for holiday accommodations or timeshares.

US-CERT also encourages users and administrators to use caution when reviewing unsolicited messages and further suggests using preventive measure to protect against phishing scams and malware campaigns. Recommendations include:

- Do not click web links in untrusted email messages.
- Refer to US-CERT Shopping Safely Online security tips.
- Use caution when opening email attachments. Review US-CERT's security tip on "Using Caution with Email Attachments" for additional information on safely handling email attachments.
- Review the Federal Trade Commission's page on Charity Scams. Use the links there to verify a charity's authenticity before you donate.
- Read US-CERT's security tip on "Avoiding Social Engineering and Phishing Attacks."
- Refer to US-CERT's security tip for "Holiday Traveling with Personal Internet-Enabled Devices" for more information on protecting personal mobile devices.

The original US-CERT release and links to more internet safety and security tips may be found on the US-CERT website.

White and Williams reminds its clients that internet security remains a critical component of any workplace policy or business operation plan. If you have questions or would like to discuss your policies and plans related to data privacy and cybersecurity, please contact Josh Mooney (mooneyj@whiteandwilliams.com; 215.864.6345), Jay Shapiro (shapiroj@whiteandwilliams.com; 212.714.3063) or Linda Perkins (perkinsl@whiteandwilliams.com; 215.864.6866).