www.privacyguidance.com
rebeccaherold@rebeccaherold.com

12 Security & Privacy Threats of the Holiday Season

1. Malicious Emails

Holiday phishing scams and malware attachments increase. A few examples:

- Notice to appear in court
- Couldn't deliver package
- Digital coupon
- "EBOLA Outbreak - FEMA Storing 250,000 Plastic Coffins"
- "Your ADP past due invoice is ready for your review at ADP Online Invoice Management"
- "I KNOW A VERY DARK SECRET ABOUT YOU. You may want to sit down if you aren't already - here it is."
- See more at http://www.huffingtonpost.com/2014/11/07/phishing-scams_n_6116988.html

2. Calls from "grandchildren" in need

- A grandchild in distress arrested and needing money, calling from a phone with bad connection
- Use info from social media (e.g., Facebook) to find those with grandchildren in teens and twenties
- See more at http://www.recorderonline.com/news/ploys-range-from-grandchild-in-trouble-to-irs/article_2a96238c-594b-11e4-9bb6-001a4bcf6878.html

3. Protect your credit card digital chip

- Keep credit cards out of sight.
- Use credit card covers with metal cover or aluminum sleeve
- See more at http://abcnews.go.com/GMA/video/tips-protect-credit-cards-hackers-26882427

4. Don't post that you're away

- Don't post to Facebook, Instagram, etc. when you're away from home and it is empty
- Don't post where you're staying while traveling
- Don't post about others either
- See more at http://www.ibtimes.com/how-burglars-use-facebook-target-vacationing-homeowners-1341325

5. Beware of USBs out of the factory packaging

- Don't use USBs in gift baskets from vendors or strangers
- Don't use USBs found in public places, on your property, etc.
- Apps download malware to USBs; don't have USB attached when using apps
- See more at http://www.engadget.com/2014/11/06/apple-malware/?ncid=rss_truncated

6. Don't purchase from unencrypted websites & bogus websites

- Look for HTTPS
- Look for a lock icon
- Beware of fake logos and trust seals
- See more at http://righton-nobull.com/blog/2014/10/know-website-secure/

www.privacyguidance.com
rebeccaherold@rebeccaherold.com

7. Fake computer security callers

- Do not believe callers claiming they need to help you remove malware
- See my experience with this in 2011 (the same scam is still being widely used) at http://privacyguidance.com/blog/cybercriminals-just-came-a-callin-at-my-house/
- See my other tips for calling scams at http://privacyguidance.com/blog/phone-scam-open-season-business-risks/

8. Be hyper-aware on social media sites

- Don't click links on a friend's wall that seem uncharacteristic; they may have been hacked
- Don't put more personal information in your profile than necessary
- Don't accept friend requests if you can't verify the authenticity of the requestor
- See more tips at http://facecrooks.com/

9. Never give your personal information to an unsolicited caller.

- Threatening to shut off power or gas if a utility bill is not paid immediately
- Claiming you must appear in court
- Targeting small businesses with invoice and phone scams
- Targeting immigrants, disables and senior citizens
- Bogus charities
- See more at: http://www.actionfraud.police.uk/news/upsurge-in-fraudsters-targeting-small-businesses-with-invoice-and-phone-scams-oct14
- See more at https://www.bbb.org/blog/?s=phone+calls

10. Malicious eCard sites

- Holiday eCards from people you don't know
- New sites for "free" holiday eCards
- Beware of cyber-ransom malware. See more at http://www.techrepublic.com/article/cryptowall-what-it-is-and-how-to-protect-your-systems/
- See more at http://phishme.com/popular-holiday-themed-phishing-attacks/

11. Malicious mobile shopping apps

- Most apps don't have effective security or privacy
- Don't allow apps access to more than they need
- Check the security and privacy of apps before using
- Check this site to see if your app has good privacy controls www.PrivacyGrade.Org

12. ATM Skimmers

- Crooks increasingly steal information at ATMs using skimming devices
- Devices over the actual ATM
- Video recorders placed in the ATM readers
- Keypad overlays
- Look at the ATM for anything suspicious and cover the keypad when entering your PIN
- See more at http://gizmodo.com/the-terrifying-evolution-of-atm-skimmers-1626794130