Online Holiday Shopping Tips

Online holiday shopping is a perfect time for cybercriminals to take advantage of unsuspecting online shoppers. Fortunately, many cyber threats are avoidable when you develop habits to protect your personal Information and keep your devices safe and secure when shopping online.

- **Shop reliable websites.**
  If an offer sounds too good to be true, it probably is! Don't be fooled by great discounts on less-than-reputable websites or fake companies. Use the sites of retailers you know and trust. Access retailers' websites by directly typing a known, trusted URL into the address bar instead of clicking on a link.

- **Beware of seasonal scams.**
  Fake package tracking emails, fake e-cards, fake charity donation scams, and emails requesting that you confirm purchase information are particularly common during this time of year. Fake communications can be in the form of text messages or email.

- **Conduct research.**
  When considering a new website or online company for a holiday purchase, read reviews and see if other customers have had positive or negative experiences with them. Also, verify that the website has a legitimate mailing address and a phone number for sales or support-related questions. If the site looks suspicious, call, and speak to a human.

- **Protect your passwords.**
  Make them long and strong, never reveal them to anyone. Do not reuse your university password on any other accounts (Facebook, Instagram, banking). Every account should have a unique password. Change your password immediately if you suspect your account is compromised.

- **Use multi-factor authentication wherever possible.**
  If you get an authentication request that you did not request, DENY the request, and report it to UHS Information Security and review your account for unusual activity.

- **Pay with a credit card, not a debit card.**
  Debit cards may not have the same level of protection against fraudulent charges.

- **Check your credit card and bank statements regularly.**
  Unusual activity is often the first indicator that your account information or identity has been stolen. If there is a discrepancy, report it immediately. Enable alerts on your financial accounts to help monitor activity.

- **Keep devices secure.**
  Regularly update computers/mobile devices with current OS versions, and software updates. This also includes devices you may use at home such as wireless routers, webcams, etc. Make sure anti-virus/anti-spyware software is installed, running, and receiving automatic updates.

- **Only use secure wi-fi.**
  Protect your data by using strong encryption on your home wireless network. Avoid connecting to public wi-fi.

UHS Information Security is working for you. We are available 24/7, to monitor and respond to time-sensitive issues. All members of the UHS community can reach the UHS Information Security Team at security@uh.edu or via phone at 832-842-4695.