Tis the season to shop, travel and boost your cyber safety

The holiday season can be hectic and, with travel, family and festivities, it can be easy to let cyber safety take a backseat. However, it’s important to always keep security top of mind: fraudsters take advantage of an increase in online shopping and traveling, and a decrease in attention, to target potential victims. In fact, U.S. online fraud attempts increased 22% during the 2017 holiday shopping season.¹ Be on the alert for suspicious emails, calls or activity, especially if the sender requests personal or financial information or requests to remote into your computer.

Ensuring cyber safety in the following key areas can help secure your personal information and help protect you against fraud:

**Travel**
- **Keep your plans private.** Do not post your intended travel plans, itinerary or location updates on social media prior to, or during, your trip. Create a social media agreement with family members to ensure they do the same, especially with children and teenagers traveling with you.
- **Use trusted travel and vacation home rental services** and only message and send funds through the site's payment and messaging tools. Don’t fall for deals that seem too good to be true; domains are inexpensive and easy for fraudsters to procure in order to create fake travel sites that capture your information—and money.
- **Avoid using public Wi-Fi** at hotels, airports, cafes and on planes, as they are more likely to be compromised or spoofed.

**Online shopping**
- **Create strong and unique passwords** across shopping and financial websites, and enable multi-factor authentication wherever offered. Consider a password management tool to help manage the passwords you have across online accounts.
- **Do not click on ads, email or pop-up links**, and type verified shopping and financial websites into the address bar instead of clicking on links from other sources.
- **Only make purchases from reputable, secure sites** (i.e., those with an https:// URL prefix); log out of websites and close the browser window after you complete a purchase.

¹ACI Worldwide, 2018
Payments

- **Treat transactions on payment apps as you would cash.** Only send money to people you know and trust, and confirm the recipient’s username/contact information prior to completing the transaction.

- **Set up online alerts on your financial accounts,** and regularly monitor your credit and debit cards and bank statements for suspicious activity.

- **Watch out for “skimming” devices on credit card readers,** and opt to use the chip reader instead of the magnetic stripe for in-store purchases. A telltale sign that a skimmer has been attached to an ATM is that the card reader is loose; ensure you shield the keypad when entering your PIN or ZIP code.

Holiday scams

- **Be wary of suspicious emails, text messages and social media posts** from people or companies you don’t know. Fraudsters take advantage of the holiday season to increase their phishing attempts, so it’s important to keep in mind that messages can include malware links or lead to online surveys that collect personal information.

- **Avoid charity scams:** During year-end giving, charities solicit donations from existing and potential donors. Always validate any change in payment instructions by calling the recipient on a known number, especially if the change is made at the last minute. Refer to [Charity Navigator](#), America’s largest independent charity evaluator, for guidelines to help protect against online scams, and ensure your donations are reaching the causes you wish to support.

- **Be careful before downloading apps for well-known retailers, financial firms and products.** Check app logos and descriptions for misspellings, missing letters or poor English, and look for other red flags, such as poor reviews, newly launched apps or links to apps from other retailers.

Remember, J.P. Morgan will never:

- Ask you to log into the same computer with more than one user’s credentials
- Ask you to repeatedly submit login credentials
- Contact you about online problems, such as logging in, if you haven’t contacted us first