‘Tis the season to avoid scams, or don’t let holiday cheers become holiday tears

by Yvonne R. Hunter | Nov 19, 2017

As we head into the holiday season, it may be a challenge to stay aware of how you can avoid being a victim of various scams and schemes to separate you from your hard-earned money.

While the topics covered may be insurance-focused, you can apply many of these cautions to other kinds of consumer transactions.

Cybersecurity

Headlines this year have been dominated by the saga of computer system hacks, made more harrowing by the Equifax breach. Insurance companies often consider consumer credit reports to determine whether you are insurable for auto and homeowners/renters insurance.

The best monitor money can buy is your own action to check your credit report on a monthly or quarterly basis. There are a number of free "credit check" report services that report on all three credit reporting organizations: Equifax, Experian, and Transunion.

Since most companies accommodate insurance payments on mobile devices, take care where you conduct these transactions. If you use a public or unsecured Wi-Fi service, you may be unknowingly sharing information with others who will gladly use it to access your information. Use your home Wi-Fi, or a password-protected system that you know has updated security. Avoid using public computers or public Wi-Fi.

Watch your email

One of the easiest ways for your information to be accessed by the "bad guys" is to allow the bad guys into your computer files and past your password-protected firewall. This is called phishing and may occur from what appears to be an innocent and safe email sent to you.

Phishing occurs when "friends" or "companies" that seem familiar to you send email messages but have odd/unfamiliar email addresses, company logos that do not match the email, etc. As a reminder, neither a respectable company nor a governmental entity will contact you to solicit your personal information without you contacting them first.

Any email that asks or insists that you change your password or personal information through an emailed link should be avoided. If in doubt about an email request, contact the company or governmental agency to confirm that it intended to send you the message.

Too good to be true

These kinds of scams generally deal with special deals or "free" money. Based on a recent search, insurance-related scams have included:

- Phishing scams related to the recent Anthem insurance cyber attacks and involved "free" credit monitoring if the recipient would provide personal and confidential information.
- Consumers contacted by contractors who provide "special" discounts to help you navigate insurance claims to recover payment for damage related to recent fire and flood disasters.
- Fake insurance brokers offering "special" discounted insurance rates. They promise insurance coverage and pocket the premium paid by those deceived into paying.

- During healthcare insurance open-enrollment periods, a caller or door-to-door salesperson will use the enrollment opportunity to start a conversation that may result in an elder or vulnerable person disclosing credit card or banking information.

If it sounds fantastic, it is probably someone else's fantasy. Consider some basic steps to protect yourself and your family.

- Take the time to research. People conducting scams want immediate action to keep you from researching who they are or information about their organization (If it exists). The "special" never existed if you are required to "act immediately."
- If you are not sure if a company representative is who they say they are, do your own research to call and confirm that the "offer" is real. An insurance company offering free credit monitoring because of a breach will have this notice on its website. Operators can also confirm whether the service is available.
- Confirm the status of any contractor's license with your local licensing office or your state's attorney general's office. Even if the contractor is licensed, ask for references and look at the work if possible. Check with the insurance company handling your claim to see if it has any past dealings with this contractor.
- Don't put personal information on public online forums. Information about your birthday, your travel plans, recent purchases (large items) and other personal information provides opportunities for identity theft and phishing.
- Insurance brokers and agents must be licensed in the states where they do business. If someone is selling insurance, check with your state insurance department or commissioner's office to confirm that the person is authorized to handle the transaction.
- Know who you are adding to your social media circle or connection.
- If you think you are a victim of a scam seek help immediately. There may be a chance to limit the harm or recover money, and you want to discourage others from falling for the same scam.

A word about travel plans

If you plan to travel during the holidays, take a few minutes to secure your residence and its contents. Some travel plans may seem to require travel insurance. You may be interested in this notice from the National Association of Insurance Commissioners (NAIC) before deciding which travel insurance policy to purchase.

The NAIC also has a handy one-page document to address auto rental insurance policies. Even if you have auto insurance coverage, you may find it worthwhile to take a minute to review this information.

By staying diligent and a bit skeptical, we can increase our opportunities for a happy holiday season.