HORIZON
WEALTH MANAGEMENT

YOUR FINANCIAL FUTURE

Your Guide to Life Planning

October 2017

Chris Dumford CFP®, AIF®
Horizon Wealth Management
699 Hampshire Rd
Suite 201
Westlake Village, CA 91361
805-446-2868
cdumford@horizonwm.com
www.horizonwm.com

CA Insurance Lic# 0A11543
www.linkedin.com/in/chrisdumford/

In This Issue

When on the Internet, You May Never Really Be Alone

Congresss action levels the playing field between ISPs, such as AT&T, Verizon, and Comcast, and Internet companies, such as Google and Facebook.

Congress has given Internet service providers (ISPs) greater freedom to use browsing activity to target advertisements and promotions at customers. The legislation (signed by President Trump on April 3) nullifies a rule that would have forced ISPs to ask for permission before tracking customers and selling their information to advertisers. The now-cancelled rule would also have required ISPs to step-up security measures to help prevent large-scale data breaches similar to those suffered in recent years by Yahoo, Target, and many others.

What's at Stake?

Congress's action levels the playing field between ISPs, such as AT&T, Verizon, and Comcast, and Internet companies, such as Google and Facebook. Historically, Internet companies have had much greater freedom than ISPs with their users' data.

Internet companies have long been collecting and using individuals' personal data to target ads at them. That's why, for example, when you research a particular vacation destination you become much more likely to see travel ads and promotions related to that destination. Now ISPs will most likely be doing more of the same.

Protecting Your Privacy

Many web browsers today have settings that allow you to conceal at least part of your web browsing activity. They can block cookies and limit websites' access to your browsing history. But web trackers are developing more sophisticated tools to monitor consumers' activity, so they can often track you even if there are no cookies to detect.

With that in mind, here are a few suggestions that could potentially help strengthen your privacy practices:

- Consider using a virtual private network (VPN) service. A VPN creates a secure, encrypted connection for data leaving your device that makes it difficult for third parties such as ISPs to monitor the content of the traffic.
- Standard ad industry opt-outs can be effective for declining ads targeted based on web surfing. If you see a triangle "I" on a banner ad, the company is offering you an opt-out.
- "Do Not Track" feature -- Web browsers may include some type of Do Not Track setting that lets you tell websites you visit, their advertisers, and content providers that you don't want your browsing behavior tracked. Selecting this setting does not guarantee that the websites you visit will honor your request. It just lets them know of your wishes.
- Use the "Limit Ad Tracking" feature on your smartphone. Generally these types of settings help users to opt out of targeted ads, but again, there is no guarantee that your data will remain private.

Finally, remember that you may have two ISPs, the company that provides broadband in your home and the company that provides wireless service to your smartphone. You should contact both of them to ask about the types of data they collect. Also ask what their procedures are for opting out of ad-targeting programs.

1-623663

The Internet Crime Complaint Center reported complaints resulting in over $1 billion in losses in 2015.

Surf Safely: Protect Yourself From Online Scams

Online criminals continuously change their operating methods. That's why it is crucial that Internet users keep up on the latest scams and the steps to take to protect their personal and financial information when online.

Here is an overview of two of the most widespread techniques being used to commit online fraud, as well as some practical tips to protect your personal security.

Phishing: This is one of the most popular methods of online fraud. Phishing, or "spoofing," is a scheme whereby users are sent fake emails that claim to be from a legitimate source. The email directs the user to a counterfeit website where they are asked to update personal information, such as passwords and usernames or credit card, Social Security, and bank account numbers. By hijacking brand names of banks, online retailers, and credit card companies, phishers often convince recipients to respond.

Crimeware: This is a class of computer programs designed exclusively to facilitate online identity theft. Cyber thieves use a variety of techniques to steal confidential data through crimeware, including:

- Secretly planting keystroke loggers onto a user's computer to collect sensitive data -- such as login and password information for online bank accounts -- and reporting the data back to the thief.
- Redirecting a user's browser to a counterfeit website controlled by the thief even when the user types the website's proper address in the address bar.
- Stealing passwords cached on a user's system.

This type of scam received national attention several years ago when it was revealed that business executives at major U.S. firms were the targets. The "bait" used to lure the recipient was an official-looking subpoena from the U.S. District Court in San Diego. When recipients clicked on the document to view it, software designed to collect keystroke data was secretly installed on their computers. It was estimated that thousands of people fell victim to this scam.

Play It Safe

The Federal Bureau of Investigation estimates that online scams were responsible for over $1 billion in losses in 2015.[1] With the number and sophistication of online scams increasing, there are some basic recommendations you can follow to help avoid becoming a victim.

- **Don't recognize it? Don't open it.** Do not open any email, email attachment, or website link from suspicious or unknown senders.
- **Don't give out your info.** Be wary of any email that asks for personal information such as passwords or account numbers. Similarly, avoid any email that promises a prize or gift in exchange for completing a survey or answering questions online.
- **Blast those pop-ups.** These small windows typically appear on or behind the window that you are currently viewing. While many are harmless advertisements, some may contain viruses or software that can monitor your Web activity.
- **Be sure sensitive data is encrypted.** Always ensure that you are using a secure website -- one that employs state-of-the-art encryption technology -- when submitting credit card data or other sensitive personal information.
- **Check your accounts.** Regularly log in to your online accounts and check your bank, credit, and debit card statements to ensure all transactions are legitimate.
- **Keep your system up-to-date.** If your computer's operating system is more than five years old it may not offer the same degree of protection as newer models. Most system manufacturers issue updates and security patches on their websites or automatically through your Internet provider. Similarly, be sure to use the latest Web browser and anti-virus software.

Finally, if you think you've fallen victim to a scam, report it. The FBI has a Cyber Operations unit devoted to fighting cyber crime. Their Internet Crime Complaint Center is at www.ic3.gov.

[1] *Federal Bureau of Investigation, Internet Crime Complaint Center. 2015 Internet Crime Report (most recent available).*

Compliance Tracking #517633
This article was prepared by Standard & Poor's Financial Communications

The opinions voiced in this material are for general information only and are not intended to provide specific advice or recommendations for any individual. To determine which investment(s) may be appropriate for you, consult your financial advisor prior to investing. All performance referenced is historical and is no guarantee of future results. All indices are unmanaged and cannot be invested into directly.

The financial consultants of Horizon Wealth Management are registered representatives with and Securities are offered through LPL Financial. Member FINRA/SIPC. Insurance products offered through LPL Financial or its licensed affiliates.

Not FDIC/NCUA Insured	**Not Bank/Credit Union Guaranteed**	**May Lose Value**
Not Insured by any Federal Government Agency		**Not a Bank Deposit**