00:00:22:01 - 00:00:57:12

Speaker 1

Welcome. My name is Andrew Baron and this is, Well... It Depends! The podcast where I present the pros and cons of different financial decisions so that you, the audience, feel better informed when you are confronted with these decisions in your own life. Well, it depends. Is sponsored by my firm, John G. Ullman and Associates. We are a team of financial planners, research analysts, tax specialists and support staff, all working together to give our clients a comprehensive experience.

00:00:58:03 - 00:01:34:21

Speaker 1

If, after listening, you'd like to discuss your situation with one of our financial planners, including me, please email info@jgua.com. In this episode I ask the question, should I be worried about my online privacy? But before we begin, a short disclaimer. This is being recorded on December 20th, 2022. The contents of this podcast are strictly for informational purposes only, and nothing said should be taken as an investment tax or legal advice.

00:01:35:13 - 00:02:07:00

Speaker 1

Any strategies discussed may not be suitable for listeners specifically, and so we strongly encourage consulting with your advisor before implementing any strategies to ensure they meet your individual objectives. Getting into it, should I be worried about my online privacy? Well... It Depends! We live in a digital world, and in fact, you are very likely listening to this on a digital device and you probably do many other things online too.

00:02:07:25 - 00:02:34:16

Speaker 1

Shopping online has become very commonplace, and many people manage their bank and other financial accounts online, and the reason for this is convenience. It's very convenient to manage your bank accounts, get holiday shopping done and watch a financial YouTube videos all from one device. But each of these log in’s and accounts present an opportunity to have your data compromised.

00:02:35:02 - 00:03:09:20

Speaker 1

Many attacks come from letting our guard down or being careless with our information, but what can you do to help? First, be on the lookout for anything out of the ordinary. You should know that the IRS will never demand gift cards for any tax liabilities, and most legitimate businesses also prefer traditional payments of cash or credit cards. Anyone demanding gift cards should immediately set off little alarm bells in your head. Close or consolidate any unmonitored accounts.

00:03:10:22 - 00:03:41:20

Speaker 1

If you have many outstanding accounts, it can be difficult to keep track of them all. And while it may have made sense to have it originally opened, it may not anymore, especially if it's unwatched. This is because software can directly target accounts that are unmonitored or inactive. Use a strong password. While you might have heard this before, it bears repeating, strong and more complicated passwords are more difficult to guess.

00:03:42:07 - 00:04:04:03

Speaker 1

And while you may originally think this has to look like a cat walked across your keyboard, instead, you can string together a list of seemingly random words such as suitcase, snow cone, door. While these are random words, they are often easy to memorize and is difficult or near impossible to guess.

00:04:06:06 - 00:04:34:07

Speaker 1

Also, use a password manager. Because we have so many outstanding accounts, it can be impossible to memorize all of these passwords. Instead, use a password manager such as automatically built in ones on many late model cell phones. Many companies offer additional layers of protection beyond the simple log in and pass code, such as having a secret word to a special question.

00:04:35:07 - 00:05:10:19

Speaker 1

The question itself may be along the lines of what is your mother's maiden name? You shouldn't answer this question specifically because this information can be looked up. Instead, you should use your own answer, like cotton candy, that would be much more difficult to guess. Two factor authentication is

another great tool. This requires the user to not only know the password, but to have access to another device like a cell phone, to grant access to the account.

00:05:10:25 - 00:05:34:03

Speaker 1

To prevent unauthorized accounts from being opened in your name, you can block access to your credit through a credit lock or a credit freeze. This must be done individually at each of the three credit agencies, but each program works essentially the same. When activated, access to your credit is denied. It is easier to lock or unlock your credit, typically done through the app and can cost money depending on the credit agency.

00:05:35:06 - 00:06:03:07

Speaker 1

Credit freezes are instead regulated federally and instead must be performed when calling into an agency with a password to freeze or unfreeze your account. To recap, there are a number of ways to prevent your data from being compromised. First, be on the lookout for anything out of the ordinary. If something feels a little wrong, it's okay to take your time and verify it before saving forward.

00:06:04:08 - 00:06:35:05

Speaker 1

If you have any unmonitored accounts, you might want to consolidate them to accounts you do watch. It's good to use technology such as two factor authentication and secret passwords to prevent the likelihood of your accounts falling into the wrong hands. Credit locks or credit freezes can prevent accounts from being opened in your name without you knowing beforehand. So to answer the question, should I be worried about my online privacy? Well... It Depends!

Speaker 1 – Andrew Baron, CFP®, EA