DEBT COLLECTORS MAY SOON CONTACT YOU BY TEXT AND SOCIAL MEDIA. HERE'S WHAT YOU SHOULD KNOW

We've all heard the stories about debt collectors hounding people. Sometimes the person owes money and sometimes its due to an error. Either way it is not easy to get it to stop.

In November of 2021, the rules for debt collectors change allowing contact by text or social media. As if the old ways weren't bad enough, now they have more ways to hound you.

You must be thinking these Insights are about cyber security. Why should I care about new debt collection changes? Because the new changes affect cyber security by providing cyber criminals with more phishing topics and more ways to get you to click on a bad link.

How? Texts and social media messages can be sent to everyone. Whether they owe money or not doesn't matter. It's just more phishing.

The message will tell them to click on a link to pay the money, or to talk to someone about setting up a payment plan, or to report an error.

The reasons don't really matter. All that matters is getting people to click on the link. And everyone falls into one of those three categories.

The new law says emails sent by debt collectors must provide a link of for you to opt out of receiving more emails. And that is good. But cyber criminals can use that as a way to get you to click a bad link.

If the debt collectors choose to use social media, they can only do it with private messaging, never a post on your site that others can see. Again, that is good. But the message must contain an opt out link similar to the emails. Links, especially ones that appear to conform to legal requirements are perfect phishing tools.

In a real message the opt out link will work to keep the collection company from running afoul of the law and you from continued communications. But for scammers, the link will take you to a fraudulent site, probably put malware on your computer, and probably make you sign in to steal more of your information.

The changes in the law spell out what legitimate debt collectors may or may not do. But for scammers, this just provides more ways to fool people into clicking bad links.

If you receive one of these messages be suspicious and never click a link. Do not call any number in the message. Never.

Find a phone number for the company sending the message by researching it on the web. See if the message is real or not and take the appropriate action then.

Want to learn more about cyber security and education, contact AIM Cyber at info@AIMglb.com or call (888) 773-1920.