Top 3 Phishing Scams Affecting Accountants

1

The Bogus Copyright Infringement Claim

The ruse: A phishing scheme that's snagged many people in its net claims that you're using copyright protected images on your website without permission. To prove their claim, all you have to do is click on a link to download the evidence. So many people think, "I don't want a lawsuit! Let me click on this link and clear this up right now.." but what happens is much worse. Instead of a copyright dispute you now have a ransomware problem.

The solution: Don't click on a link in an email from anyone you don't know. If you receive an email like this and you want to make sure there's no real issue, check with your website developer. Any reputable developer will have purchased your website images through a licensing agreement with a stock photography agency like Getty Images.

2

The Fake Domain Invoice

The ruse: Many people don't remember where they bought their domain or who is responsible for renewing it. Online scammers take advantage of this and use it as bait to scare people into paying fake domain renewal invoices. If you get an email threatening that your domain will "terminate in 24 hours", don't panic and don't pay. Your domain registrar will never send you an invoice attached to an email and they will never try to charge you the $100 or more per year (the average renewal is only around $10-20 a year).

The solution: To put your mind at ease, contact your website hosting provider for the quickest answer. They should easily be able to tell you holds your domain and when and how it should be renewed.

To check it out yourself, go to https://who.is/ and type your domain in the field provided at the top. The information returned will include the "registrar" or company where your domain was purchased like GoDaddy, Google Domains, Network Solutions, etc. It will also clearly tell you what date your domain expires. If you really do need to renew your domain, login to your registrar account to complete the renewal process.

3

The Email Upgrade Scam

The ruse: Without email, your small business is dead in the water. Online scammers capitalize on this fact to try to make you believe that your email account is somehow about to "expire" and all you have to do is enter your password in order to login and fix the problem. They'll often frame this petition in an email that looks legit at first glance. The message might be written with proper grammar and professional language and will appear to come right from Microsoft, Google, or your website hosting provider, even using their logo. Fearing a world without access to email, you could walk right into the jaws of a scammer.

The solution: If you receive an email asking for a password, don't send it! Your email or website hosting provider will never request this info in an email. To be on the safe side, forward the message to your IT company or website hosting provider and ask them if there are any real issues with your email account.

At Build Your Firm, we're always looking out for our clients and our team is ready to answer questions about emails, domains, and websites. If you're interested in building a new website, check out our accounting websites or call **888-999-9800 ext. 1** now.

Build Your Firm®
Work Smarter, Not Harder!