HUDOCK CAPITAL GROUP, LLC
WEALTH PARTNERS WITH PURPOSE®

Imagine this scenario. You get an email that appears to be from your bank. You open it and read a message riddled with misspelled words that direct you to "click the link below." You click on the link and are taken to a page that looks *almost* exactly like the website you're used to visiting.

Almost.

This type of scam is what's known as *phishing*, and hopefully, it's never happened to you. Or, if it has, hopefully you recognized the warning signs and knew to stay away. Unfortunately, many people *don't* recognize those signs, and fall prey to a particularly insidious form of fraud that can be very damaging to your finances.

To help you understand more about what phishing is, and how you can protect your finances from it, we have prepared a special list. It lists some of the common ways hackers try to "phish" for your personal information and provides some common-sense rules that will help increase your cybersecurity.

## Tips to Protecting Yourself from Scammers…

**Contact Information**

Make sure the contact information you're using to send money has been enrolled by you at the financial institution and is linked to your account before sending money to yourself. Scammers may contact you pretending to be your financial institution telling you that they noticed suspicious activity on your account. They may ask you to send money to yourself to "reverse" the payment.

**Personal Information**

If you receive a call from your financial institution asking you to provide personal information or to transfer money and you aren't sure if the call is legitimate, it's best not to provide any information and to call the phone number on the back of your debit/credit cards or on your bank statements.

**Utility Companies**

If a utility company calls to tell you that your electricity payment is past due and wants to collect a payment, it's best to call your utility provider before making the payment via phone. Your utility providers will send you letters or emails before a situation gets serious.

**Support Specialists**

If you need support from a company such as Comcast or Amazon, be sure to call the company using a reliable number. Scammers may pretend to be support specialist from well-known companies in order to gain access to your information. Never click on a link that they provide or download an app that they suggest. Remember, they'll never cold call you.

## …and How Hudock Capital Group Keeps Your Information Safe

**Network Security**

Hudock Capital Group employs an IT Technology Specialist to manage systems internally. We utilize a multi-faceted security approach to our network, email, hardware, and software. Some of these security measures include, but are not limited to, enterprise-level site firewall that is monitored and kept up to date by a third-party technology provider, up-to-date anti-virus/anti-malware solution, data protection backup via Carbonite, controlled access to data, multi-factor authentication, and systems to provide for updates and fixes for Windows and other third-party application.

**Practice Management Security**

Hudock Capital Group uses Redtail Technology as the firm's practice management software. Redtail Technology is a "Cloud" based service where software and data are centrally hosted and accessed by the firm using a web browser and internet connection. Redtail Technology uses the secure Amazon Web Services (AWS) infrastructure to provide a secure platform. Additional information regarding the security specifications of AWS can be found by visiting https://aws.amazon.com/compliance/shared-responsibility-model/.

All data transmitted between our vendors and the firm is encrypted via HTTPS. Hudock Capital Group also uses Smarsh Encrypt when sending sensitive information via email. This service sends an encrypted email which requires the recipient to log into a secure website to open the email.

**Employee Training**

All employees at Hudock Capital Group receive regular security awareness training on cyber security topics such as phishing, creating strong passwords, ransomware, suspicious emails, and mobile device security. Staff computers and email are password-protected and monitored regularly for malware. Additionally, all employees must complete a background check prior to employment, agree to the firm's confidentiality policy, and receive training on how to handle sensitive client information.

We hope you find this information helpful. Additional questions regarding data security can be directed to Wayne Dieffenderfer, Chief Compliance Officer, by calling the office or emailing wdieffenderfer@hudockcapital.com.

Sincerely,

Barbara B. Hudock, CIMA®, CPM®
Chief Executive Officer
Founding Partner

Michael J. Hudock, Jr., CPM®
President and Founding Partner
Wealth Consultant