LINDQUIST VON HUSEN & JOYCE LLP
Certified Public Accountants

Insights
News | Resources | Perspectives

Simple Reminders & Steps to Protect Your Accounts From Identity Theft & Fraud

Today we live in the world running on the Internet and technology 24/7. With the speed and convenience, technology also brought us unprecedented risks, especially when it comes to how our personal and business-related financial information and transactions are recorded.

Do you shop, pay bills, post updates on social media sites or get electronic boarding passes online or use mobile apps to do all those? Do you tend to use the same passwords or PINs for multiple accounts? Have you given up your personal information to enter for sweepstakes or contests? Do you wait until last minute to file your tax returns?

If you answered "yes" to any of these questions, you are completely normal – but consider being at risk for online fraud. Even if you answered "no" to all, you are still not safe and should take precautionary measures to protect your identity and your accounts.

Simple Protection Efforts Go a Long Way

The Federal Trade Commission (FTC) offers these recommendations to safeguard your personal and financial data from unauthorized hacking (Learn more here):

- **When in doubt, do not respond online:** Unless you initiated the contact or know the person or company you are dealing with, do not give out your personal contact or biometric information online. If you are unsure of the legitimacy of the email you received, try calling the customer service instead of replying to the email or clicking on links in the email.
- **Dispose of technology devices safely:** Use a wipe utility program to overwrite the entire hard drive and remove your personal information and your contacts before throwing or giving away your old cell phones.
- **Encrypt your data:** Consider using encryption software to protect your online transactions. Look for the "lock" icon on the status bar of your browser before you send personal or financial information online.
- **Make your passwords complex:** Use a special phrase or the first letter of each word for your password or combine symbols, numbers, and upper and lower case letters to create long and "strong" passwords.
- **Limit your social networking network:** If you frequently post updates about yourself and your family on social media sites, limit access to your networking or profile page to a small group of people you trust.

The Internal Revenue Services (IRS) also warns taxpayers about tax-related scams (Learn more here):

- Try to file your tax return early in the filing season — before an identity thief beats you to it and claim a fraudulent refund, using your personal information.
- If you receive a notice from the IRS, respond immediately to the name and number printed on the notice or letter. If you believe someone may have used your Social Security number fraudulently, you'll need to fill out IRS Form 14039, **"Identity Theft Affidavit."**
- Remember that the IRS does not call individual taxpayers directly. In case you receive a call from someone pretending to be an IRS officer, hang up and report to the IRS.

If you have any questions or concerns regarding the safety of your financial data, please feel free to contact **Cathy Hwang**, Partner, at *chwang@lvhj.com* or 415-905-5436.

Click here to read more about Cathy Hwang.

LvHJ Insights is an e-newsletter of Lindquist, von Husen & Joyce LLP designed to share firm and industry updates, useful resources and perspectives on current issues that are important to its clients and business leaders. We welcome your feedback.Call us at 415-957-9999 or email us at info@lvhj.com.