What is Phishing?
How to Avoid Getting Hooked

Phishing emails look like regular, legitimate email, often coming from someone in our contact list. The emails are usually very general in information and are often asking us to take action by clicking on a link or calling a phone number. The email may:

- promise a reward
- threaten a punishment
- appear mundane

The email can also look like it is coming from a company or organization that we do business with. For example, email scams have gone out that are made to look like they are from Schwab, the Better Business Bureau and the IRS, just to name a few.

Remember, any email that looks even slightly suspicious should be deleted. If we think it may possibly be legitimate, pick up the phone and call the sender from a phone number that we already have in our contact list, NOT the one being provided in the email. Verify that the email or information is legitimate. Read through the following Do's and Don'ts and read the Additional Resources for more helpful information.

DHJJ FINANCIAL ADVISORS

Avoid Getting Hooked by a Phishing Scam

Do

- Read email with a cautious eye as Phishing scams are becoming more and more sophisticated
- Confirm something that seems suspicious by calling the company or contact person directly from a phone number already in our possession
- Make sure a website that we are using to make a purchase has “https” in the URL and a small lock icon on the address bar
- Remember that legitimate companies will never try to solicit financial or personal information over email
- Be wary of Pop Ups
- Install and keep antivirus software up-to-date

Don’t

- Send money to someone we have never met face-to-face
- Click, download or open anything that comes from an anonymous sender or looks even slightly strange
- Believe everything you see
- Buy online unless the transaction is secure
- Share personally identifiable information with someone that has contacted you unsolicited, whether over the phone, email or social media
- Use untraceable transactions such as solicited wire transfer or cash-only deals

DHJJ FINANCIAL ADVISORS

Additional Resources

- U.S. Securities and Exchange Commission https://www.sec.gov/reportspubs/investor-publications/investorpubsphishinghtm.html

- Anti-Phishing Working Group https://www.antiphishing.org//

- Better Business Bureau: 10 Tips to Avoid Scams https://www.bbb.org/avoidscams

DHJJ FINANCIAL ADVISORS