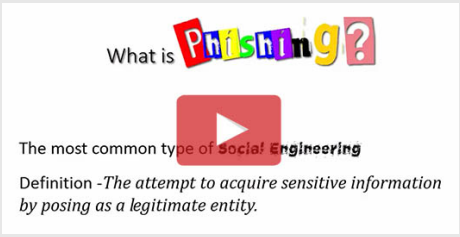
The News You Need to Know

Left to right: Andrew Woolley, Andrew Barninger, Christopher Miller, Stephen Bell and Alan Loss.

Watch this video to learn more about phishing and how to protect yourself:



The Recent Rise in Identity Theft

Steps to defend yourself.

Many of our clients have expressed concern about the recent rise in identity thefts. If you're concerned, here are some steps you can take to help defend yourself.

Don't trash it; shred it. Shred anything financial, aside from your tax records: credit card statements, bank statements, old checks, deposit slips—you name it. A cagy thief can borrow thousands of dollars or order checks in your name with such data.

If you don't want to spend time shredding them yourself, you can pay to have it done – there are office supply stores that now offer the service. If you really must keep these periodic records, hide them in the most unvisited place possible.

Hide your Social Security card. The only time you need to show it to anyone is when you start a new job. Otherwise, there's no need to carry it around.

Don't buy things through obscure websites or payment services. If you've never heard of the company or the payment method used by the seller, don't take the risk – or, at the very least, do some Googling to see if there have been any identity theft problems linked to the seller or the payment engine.

Learn to recognize a phishing attack. Phishing is when an identity thief sends you an email message that mimics a legitimate communication from a credit card firm, bank, or government agency. Skillful phishing scams a recipient into handing over account passwords and confidential personal or financial information. Phishing is also becoming increasingly common on smartphones, and on social media hubs.

How can you spot a phishing scam? First of all, credit card companies, banks, and government agencies will never ask you for your password or account info by email – so if you see this, it is a red flag. Phishing emails usually tell you your account is going to

Personal Wealth Advisory, LLC
Wise strategies for your wealth and your life

630 Delp Rd., Suite 100
Lancaster, PA 17601
p: 717.735.1170 f: 717.735.1181
www.pwallc.net
info@pwallc.net

Securities offered through Geneos Wealth Management, Inc. (Member FINRA/SIPC). Advisory Services offered through Personal Wealth Advisory, LLC and Geneos Wealth Management, Inc. a Registered Investment Advisor.

© 2017 Personal Wealth Advisory, LLC. All rights reserved.

be closed, or they promise you a big gift. They try to lure you to an unsecured website. A truly secure site address always begins with https://, and your browser should show an icon of a closed lock in the upper left-hand corner.[1]

Ask for an annual credit report from Equifax, TransUnion, and Experian. These are the three American credit reporting agencies. Get an annual report from each of them; you are legally entitled to download one free credit report per year from each bureau. This will tell you if someone else has opened an account in your name.[2]

Citations:
1 - halewebdevelopment.com/10-tips-to-prevent-phishing-attacks/ [7/20/16]
2 - fool.com/knowledge-center/credit-essentials-what-you-need-to-know.aspx [8/21/15]

Securities offered through Geneos Wealth Management, Inc. (Member FINRA/SIPC). Advisory Services offered through Personal Wealth Advisory, LLC and Geneos Wealth Management, Inc. a Registered Investment Advisor.

© 2017 Personal Wealth Advisory, LLC. All rights reserved.