Hello. My name is Allan Pomerantz and I have been your neighbor in Hershey's Mill for a little over a year. In my last position I was the Chief of Computer Security for the Philadelphia Stock Exchange until it was bought by NASDAQ. It was my responsibility to protect the Exchange from being hacked which fortunately was the case.

In doing this job I also spent a lot of time learning about on-line frauds, scams, and methods crooks use to access your computer and relieve you of your money. My files on these topics are unfortunately quite large. Also, another unfortunate issue is that many of these attacks are aimed at retired and elderly people primarily because their success rate rewards the fraudsters sufficiently to keep at it.

Now that I am both retired and a resident of HM, I would like to share this information with you in on-going series of free E-Mails. To continue to receive your copy of this newsletter all you need to do is to reply to this E-Mail and I will put you the distribution list. I have no intention of ever charging for this or selling anything.

What follows is the first newsletter. Future issues will be based on the interest that you folks express and other important topics as well as scams you report to me.

INITIAL NEWSLETTER

ALERTS AND TIPS TO PROTECT YOURSELF FROM BEING SCAMMED

This newsletter will deal with four scams that are very prevalent right now. The first is a perennial because it's Medicare Open Enrollment time. The second is just the opposite because scammers like to deal with current events so it is related to Ebola which is on everyone's mind. The other two involve a recurrent one - a fake internet coupon from Kohls while the last one is for people who own timeshares.

Medicare Open Enrollment - Oct 15th to Dec 7th

What are they looking for?

Your medicare number which is also your social security number

Your Bank Account Number

How will they trick you into giving it to them?

They will call or E-Mail you saying Medicare needs your number so they can issue a new card. That is not true because Medicare already has your number and banks and government agencies no longer ask you for such information.

To get your bank account number they may threaten your medicare coverage because of an overdue bill or missed premium that you must pay immediately.

What should you do?

If it's a phone call hang up instantly.

If it's an E-Mail asking for your medicare number hit the DELETE button immediately.

BONUS – Tips From Consumer Reports to Further Protect Yourself

Caller ID is completely untrustworthy. Crooks can display any number / Name they want.
You normally don't need supplemental medicare insurance especially from someone you don't is pressuring you to buy.

This piece of advice applies to every financial thing you have -medical insurance, credit cards, bank accounts, etc, Review anything you get from Medicare, doctors, banks that deals with activity in your name This is key to limiting the damages if you are a victim.

Always assume any offer of FREE medical supplies is a scam and hang up. Remember that no legitimate business can operate giving their product away free.

Don't help fraudsters by agreeing to accept or just sign for unneeded care or get involved with a crooked billing in exchange for a kickback . First, keeping Medicare costs down helps keep Medicare available. Second, if you help fraudsters you are a fraudster and can go to jail or pay heavy fines.

Ebola Scams.

Scammers prey on fears during the worst of circumstances – and the Ebola crisis is no different. Fraudsters are already using sleazy tactics to turn a quick buck.
The U.S. Food and Drug Administration has seen and received “consumer complaints about a variety of products claiming to either prevent the Ebola virus or treat the infection.” Despite these claims, “…there are no approved vaccines, drugs, or investigational products specifically for purchase on the Internet.” And the Council for Responsible Nutrition, a trade association for the dietary supplement industry, warns consumers that there are currently no supplements that can prevent or cure Ebola.

What to Look Out For

online offers for an Ebola cure or special “natural” or “dietary” methods to alleviate or prevent symptoms

email scams with alarming messages like "Ebola update"or “Ebola Pandemic” which may include links that release computer viruses
sales of "personal protection kits"at low prices to provide supposed “infection defense”

charity scams claiming to help victims or fight the disease

potential stock investment frauds involving companies that say they are involved in the development of products that will prevent the spread of viral diseases like Ebola.

What Should You Do?

delete any suspicious emails without opening or clicking on any links

ask how donations will be spent and check a charity’s legitimacy on the Charity Navigator website

before providing any money

never provide your personal or financial information to companies you don’t know

What if I Have Questions?

If you have questions about a possible Ebola-related scam, contact:

State Attorney General: naag.org
Food and Drug Administration: fda.gov
Centers for Disease Control: cdc.gov
Federal Trade Commission: ftc.gov

Kohl's Gift Card Scam

Claim: You can receive a $100 Kohl's gift card by following three simple steps on Facebook.

Fact: In October 2014, a survey scam tempting Facebook users with a free $100 Kohl's gift card began spreading like wildfire.
It would be easy to mistake the Kohl's $100 gift card scam for the real thing, as the page to which users are redirected appears to be both legitimately branded by Kohl's and nearly identical to some Facebook pop-up "like and share" functionality. However, the page to which users are taken is actually not a part of Facebook and simply mimics the look and feel of a genuine Facebook like/share prompt.Unfortunately, more than six million Facebook users have fallen prey to the scam. Many wary customers have taken to the official Kohl's Facebook page to warn the company of the well-trafficked scam

Scams Against Timeshare Owners

Advance Payment Or Special Promotion Scam:

The scammer might ask for an advance payment or deposit via wire transfer. In these circumstances, the service they claim to sell is never rendered. The request for payment is not always immediate. They may work with you over a period of time, gradually gaining your confidence. It is usually a "closing cost, deposit, processing fee, tax, transfer fee or a fee to clear a title defect" that is requested in advance.

Identity Confusion to Redirect Payments Scam:

Unlicensed and illegitimate persons sometimes attempt to pass themselves off as timeshare representatives, and may even claim to be an employee, agent or affiliate of your timeshare company. They may contact you by phone, general mail and email in an attempt to redirect payments or provide alternative payment information similar to the "COMPANY NAME Payments" name, address, or website. The payment information they may give to you may vary by just one letter or digit in a P.O. Box number, bank account, or web address. On written or web communication, they may use unauthorized replica logos from your company or one of their resort hotel brands.

Escrow Or Clearing-House Scam:

Scammers may assure you of the safety of your transaction by instructing that your payments be made to a "clearing house," a "processing center," or even into "escrow with a title company." All may be fraudulent names or addresses used by the scammer. Please be aware, your timeshare company usually does not accept payments via "direct withdrawal from checking Account (check by phone)," "Western Union" or "PayPal." On your invoice, you can find a list of the accepted payment methods.

Immediate Action Required Scam:

A scammer may state that you must act immediately or without delay. The due date for payments to Your timeshare company is always written on your invoice. If anyone suggests that you respond or make payment by a different date, contact your customer service department immediately. Make all contact, communications and payments exclusively through the channels provided in your contract documentation or on your invoice. If you receive unsolicited or suspicious communications about your membership

That's it for this newsletter but there's much more to come as scammers never rest.

Allan Pomerantz