SPRING 2016 HERSHYSMILL FRAUD PREVENTION

NEWSLETTER #7

Spring has sprung. The grass is riz. I wonder where the flowers is?

OK. So Longfellow doesn't need to worry. I'm no poet but I bet I know more security than he did.

So once more into the breach.

SMARTPHONE SCAMS

Now that nearly everyone has a smart phone scam, artists are heeding Willie Sutton and going where the money is, which in this case is your smartphone. How big is the problem? AARP estimates that over 25% of text messages offering free gift cards or lower priced drugs are criminal attempts to defraud you. My guess is it's much higher than that.

There are really two types of smartphone scams.. The first group which we've covered previously are not specific to smartphones. They work on any phone and are such things as the grandchild scam.

The second kind are more directed to smartphones.

SPAM TEXTS.

These are more frequent than on your computer because for some reason people are three times more likely to respond to a phone spam than an E-Mail spam message. The main objective of these messages is to get you to click on the included link which will take you to a bogus website. Once there it will install spyware designed to steal credentials and passwords. This works very well because smartphone security is very much less protective than your computer's security.

WHAT TO DO.

First, if you think it's spam, don't open it, just delete it. If you open it don't click on any links. Most important, DON'T fall for the OPT OUT button to stop these E-Mails. You will get a double hit. First, you'll be going to their

bogus web site. Secondly, you will be tagged a pigeon and will receive even more spam.

ONE RING SCAM

The ruse here is to robocall thousands of smartphones, ring once, and hang up before you can answer. The hope is that you will be so curious about who called that you will dial back. When you do you will be calling a foreign number that charges a premium ($20+) per minute and you will be put on hold and transferred around until you hang up. These charges then appear on your phone bill with bland descriptions such as *special services* in hopes you won't notice.

WHAT TO DO

If they don't leave a message just delete the number. If they do leave a message see if they call you again.

BANK MESSAGES

The classic fake bank message says there is a problem with your account and you must click on the link to address it. The fake website will look as much like your bank as the crooks can make it (usually pretty close) and you will asked to give them your user ID and password when you LOGIN.

WHAT TO DO

Delete this message immediately and call your bank using the number from their website that *you* opened yourself.

A FINAL TIP.

Losing your smartphone can be very damaging so use a pin that's not easy to guess and don't store financial credentials on it. Yes, this means you won't be able to bank by phone which you don't need unless your name is Warren Buffet.

PHONY IRS CALLS

I know this a repeat but please indulge me. I'm doing because given the time of year and the devastating financial consequences of falling for this one. In fact, this scam increased 2000% between 2013 and 2014 targeting 54,000 Americans.

THE THREAT CALL

Basically, the caller says he's with the IRS and you owe delinquent taxes and if you don't pay immediately you will go to prison, your house will be taken etc. This of course is nonsense. If you need iron-clad proof it's a scam you will be asked to send money in an untraceable, unrecoverable personal way. The IRS will inform you in writing if you owe back taxes and an interactive process will take place

THE VERIFICATION CALL

Although the goal is the same, the technique is different. Instead of a threat, the caller says he's with the IRS and needs to verify some information to process your return. They may use **Caller ID Spoofing** to show the call is from the IRS. They also may use official IRS job titles and fake badge numbers.

WHAT TO DO

Hang up. Ignore the caller. If you were contacted by phone report the call to the Treasury @ **800-366-4484**. If by E-Mail forward it to **phishing@irs.gov**

DEBIT CARD TIPS

In general, it's safer to use credit cards than debit cards. Your fraud protection is stronger ($50) with no time limit. With debit cards the $50 limit is only good for two days. If you do not report the charge it increases daily for 60 days after which there is no loss limit. But some people prefer the discipline of a debit card and some places may take only debit cards but. At

any rate, here are a few debit card tips.

Choose the **Credit Option** if available. The money comes out of your account but you get credit card protection. You may have to sign but so what?

If the credit option is not available **LIMIT USAGE** to places where a clerk is always present to reduce the danger of a **SKIMMER** installed in the machine which will steal your card number and pin.

Finally, if you don't use your debit card for purchases ask your bank for an **ATM ONLY** debit card. You can get money from an ATM with your pin but it cannot be used otherwise.

CHIP CREDIT CARDS

While the new chip cards are a vast improvement in security, no good deed goes unpunished. The scammers are sending out realistic phishing E-Mails that you have to fill out to get a new chip card. So if you respond they won't have to worry about the chip security. They'll already have all they need. You don't have to do anything to get your chip card. The bank will just mail you your new card when its ready.

FAITH BASED DATING

The sites themselves (Jdate, Christian Mingles) are legitimate but scammers are registering to relieve people who are looking for love of their money. Remember, people looking for mates should not ask for money. Also, to avoid creepy characters check them out on spokeo.com and validate their address on Google maps.

GRIEVING WIDOW

THE SCAM

Anyone who has just lost someone is not in a good state to avoid being scammed. Despicable con artists read the obits and then pretend to be

from the bank to swindle the bereaved.

WHAT TO DO

If it’s you ask someone you trust to handle your financial affairs until you feel confident enough to take over. Especially ask them to be aware of suspicious E-Mails or phone calls.

If it’s someone you care about, volunteer to do it for them.