Know The Threats To Help Protect Your Identity – SMiShing

Similar to phishing, SMiShing uses cell phone text messages to deliver the "bait" to get you to divulge your personal information. The "hook" (the method used to actually "capture" your information) in the text message may be a web site URL, however it has become more common to see a phone number that connects to automated voice response system.

The SMiShing message usually contains something that wants your "immediate attention". Some examples include:

1) "We're confirming you've signed up for our dating service. You will be charged $2/day unless you cancel your order on this URL: www.samplecompany.com."
2) "(Name of popular online bank) is confirming that you have purchased a $1500 computer from (name of popular computer company). Visit www.samplecompany.com if you did not make this online purchase."
3) "(Name of a financial institution): Your account has been suspended. Call xxx-xxx-xxx immediately to reactivate."

The "hook" will be a legitimate looking web site that asks you to "confirm" (enter) your personal financial information, such as your credit/debit card number, CVV code (on the back of your credit or debit card), your ATM card PIN, SSN, email address, and other personal information. If the "hook" is a phone number, it normally directs to a legitimate sounding automated voice response system, similar to the voice response systems used by many financial institutions, which will ask for the same personal information.

Do not respond to text messages, website addresses or telephone numbers that may warn of dire consequences unless you validate your information immediately. Contact the company to confirm the text validity using a telephone number or Web address you know to be genuine. Primary Bank will never ask you for your PIN number.

“Please visit www.onguardonline.gov for more practical tips from the federal government and the technology industry to help you guard against fraud and protect your personal information.”

“Have you fallen Victim to a Phishing or SMiShing scam?

www.IdentityTheft.gov offers a step-by-step checklist of what to do right away and guides you on what to do next. You can file a complaint with the Federal Trade Commission (“FTC”) by visiting www.ftc.gov/bcp/edu/microsites/idtheft/ or by calling (877) ID-THEFT (877-438-4338).

If you have responded to an email or text message that you suspect may be fraudulent, contact your bank immediately so they can protect your account(s) that may have been compromised. You will probably need to close the account(s) and open a new one(s) to ensure safety of your information.

If you shared your Social Security Number, you will also want to notify the three major credit reporting companies: Equifax, Experian, and TransUnion in order to help salvage any damage that may come from having it exposed to one of these (or any other) fraud scam.