The Monthly Brief

Volume 5 Issue 5 May 2017

What Is Smishing?

We've warned you about phishing emails, but there's also a text message version called "SMishing," short for SMS phishing.

The texting scam looks legitimate because it pretends to be a fraud alert from your bank or credit card issuer.

Scammers are spoofing banks' phone numbers and sending text messages. A spoofed phone number hides the actual number the text is coming from and displays a number from a trusted source, like your bank.

The text claims that your debit card or account has been restricted or used to make a purchase and if you do not recognize the transaction, to call their fraud prevention helpline.

A linked phone number is provided for you to call. Calling the number provided in the text connects you to the fraudster who will then ask you to confirm your sensitive banking details. With this information they can steal money from your account.

In at least one reported incident, when the victim notified her bank, the claim was denied. The bank said that it was not at fault because the victim willingly divulged personal security information used to obtain money from her account. While we don't believe this is the norm, it's worth considering.

To learn more and get tips on how to avoid SMishing attacks, visit our Facebook post by **clicking here**.

Follow Us On Facebook

Subscribe: philarcher@sa18.org

DATA BREACH...AGAIN!

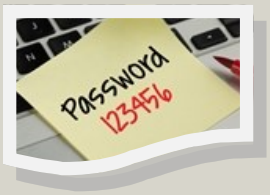
International Hotels Group (IHG), the parent company for over 5000 hotels world wide, including Holiday Inn, Intercontinental, Crowne Plaza, Staybridge Suites, Kimpton Hotels, Even Hotels and Hotel Indigo, is reporting a major data breach.

Over 1,200 IHG branded franchise hotel locations across the U.S. and Puerto Rico have been hit with payment card stealing malware. Anyone who stayed at an affected property between September 29, 2016, and December 29, 2016, potentially had their payment information stolen.

IHG didn't report this until March 2017 so its probable the breach continued till then. Stolen information included the cardholder's name, card number, expiration date and internal verification code.

Click here to visit a page set-up by IHG that lets you search for affected hotels. Use the drop boxes to locate hotels and if one you've visited is on the list, your financial data may have been stolen. If so, immediately contact your financial institution and change your online account login information.

Creating Secure Passwords



You've probably heard that secure passwords require long strings of random letters and symbols that are nearly impossible to remember. However a study by Carnegie Melon University has shown that unique pass phrases with a personal meaning can be just as effective.

To construct our easy to remember password, we'll use the phrase **"Fly me to the moon"**. Taking the first letter as a capital and the remainder as lower case, it converts to **Flymetothemoon.**

Next, add a unique way to customize it for each website. We'll use the at "@" symbol followed by the capitalized first and last letter of the website name. So for Amazon our password would be **Flymetothemoon@AN**. For JC Penny it would be **Flymetothemoon@JY**.

Another technique is to use the first and last letter of each word in your phrase. In our case it would become **Fymetotemn@AN** or using alternate capital and then lower case letters it becomes **FyMeToTeMn@AN**.

Using variations on these simple techniques can provide you with easy to remember very secure passwords for every site you do business with.