INFORMATION SECURITY & YOU | 2nd Quarter 2014

Up-to-date information on privacy & preventing identity theft and financial fraud

Powerful Passwords

Strong passwords and password management systems are powerful tools in the war against identity theft and fraud. They could mean the difference between your information being compromised at one merchant versus your information being compromised across all of your banking, social media, retail and other online accounts. By following the steps below, you are likely to reduce your risk of identity theft or financial fraud.

1. **Create strong passwords.** At a minimum, all of your passwords should be eight (8) characters long, and should have at least one of each of: lower case letters, upper case letters, numbers, and special characters. Also avoid using the word "password", 1234, your or your family's names or birthdates, or other easy to come by information about yourself in the password.
2. **Create unique passwords for ALL of your accounts.** We know this sounds difficult, but with the recent spate of data breaches, the heartbleed bug, and evolving malware, online security is at an all time low. This step could keep a small loss from turning catastrophic. If you're having a hard time coming up with your passwords, you can try a password generator like the one found on the Norton website: *https://identitysafe.norton.com/password-generator#*
3. **Use a password management system.** Whether you use an encrypted Word doc or use a password management app on your mobile device, this can be a life saver! Just remember to research before you buy, and securely back up your information.
4. **Change your passwords often.** The word "often" is a vague term, but the idea here is to not use the same password forever. Figure out what is a reasonable timeframe, and stick to it.
5. **Don't use the "remember password" option.** Although it's convenient, having the browser or other application set up for automatic login means that anyone with access to your computer has access to your information and accounts.

Consumer Financial Protection Bureau Issues Elder Exploitation Prevention Manual

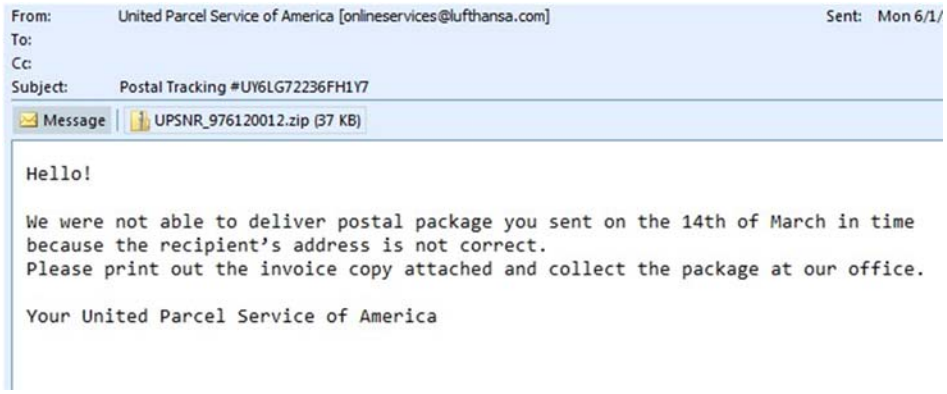
The CFPB has created a manual to help nursing homes and assisted living facilities protect, detect and respond to vulnerable adult abuse and exploitation. This new publication can be found at:
http://files.consumerfinance.gov/f/201406_cfpb_guide_protecting-residents-from-financial-exploitation.pdf

Social Engineering Basics – Part 2

In the last issue, we introduced you to social engineering and how it is a key part of fraud methods. In this issue, we want to give you some actual examples of the most common form of social engineering—phishing. Whether it's straight phishing using mass mailed e-mail, vishing using voice mail, or spear phishing by sending out directed email to specific groups of people, phishing continues to plague consumers and businesses alike. We all receive so many messages and have so many online accounts, that it's very easy to accidently think you are accepting a friend request or opening up a file full of pictures from your great aunt Agnes. The biggest threat posed by phishing is the apparent legitimacy of the messages sent, and the often urgent call to action posed by the fraudsters. Here's some examples:

Look for what's wrong with this email:

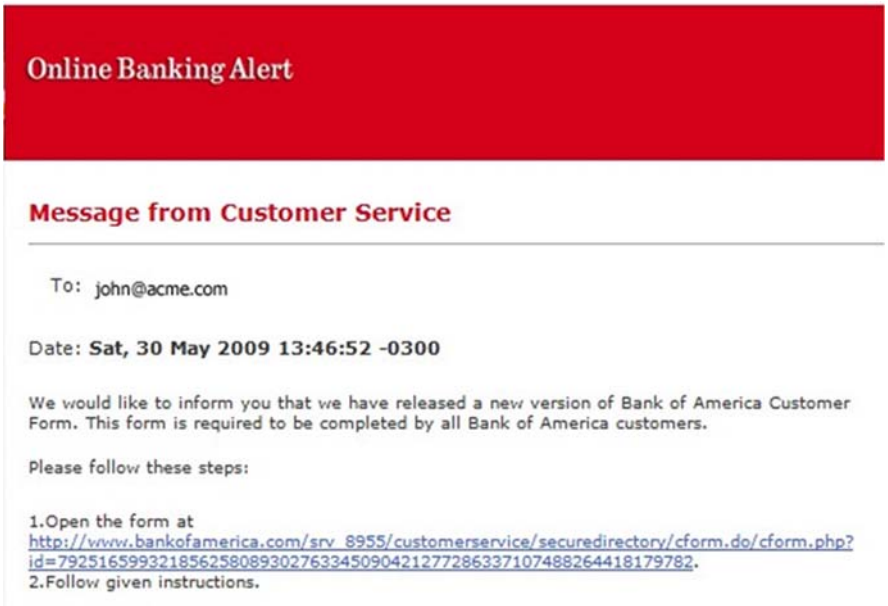
1. It's not addressed to you by name.
2. The From address is nonsense.
3. You're being asked to open a .zip file.
4. The zip file contains a .exe file that's most likely malware .


From: United Parcel Service of America [onlineservices@lufthansa.com] Sent: Mon 6/1/
To:
Cc:
Subject: Postal Tracking #UY6LG72236FH1Y7
Message | UPSNR_976120012.zip (37 KB)

Hello!

We were not able to deliver postal package you sent on the 14th of March in time because the recipient's address is not correct.
Please print out the invoice copy attached and collect the package at our office.

Your United Parcel Service of America


Online Banking Alert

Message from Customer Service

To: john@acme.com

Date: **Sat, 30 May 2009 13:46:52 -0300**

We would like to inform you that we have released a new version of Bank of America Customer Form. This form is required to be completed by all Bank of America customers.

Please follow these steps:

1.Open the form at
http://www.bankofamerica.com/srv_8955/customerservice/securedirectory/cform.do/cform.php?id=792516599321856258089302763345090421277286337107488264418179782.
2.Follow given instructions.

Look for what's wrong with this email:

1. It's not addressed to you by name.
2. There is no indication that the sender knows your account information.
3. You're being asked to click on a link and give personal information.
4. When hovered over the link goes to a bogus site.

Just remember the best way to protect yourself is to think before you click—don't automatically click on email attachments or links. If the message appears to be from a legitimate source, go to your browser and enter the company's web address yourself, and look to see if the site is secure (look for the https:// or lock icon). For more information, check out these great resources:

OnGuardOnline.gov | *http://www.onguardonline.gov/phishing*

Stop. Think. Connect. | *http://stopthinkconnect.org/tips-and-advice/overview/*

StaySafeOnline.org | *http://staysafeonline.org/stay-safe-online/keep-a-clean-machine/spam-and-phishing*