

Computer Safety

Howard Verne

4/12/2018

Is My Private Information Safe?

NO!!

- Millions of people's Information has been stolen to date
 - Panera Bread, Saks, Experian, Yahoo, Uber, Target, Home Depot Even Albertsons have been some of the largest/well known break-ins
 - You really should check if your Facebook data was stolen by Cambridge Analytica, users should start seeing one of two messages at the top of their Facebook feed with the header "*Protecting Your Information*".
 - Information stolen includes email addresses, credit card information, and passwords
 - Using the same passwords on several sites is a *bad/dangerous* practice
 - This information is for sale on hacker sites (typically \$5-6 per person)
 - The average website gets attacked 44 times a day

What should I do?

- Be paranoid!!
 - Check your credit card statements carefully
 - Hackers have gotten smart they often just charge small amounts to your card
 - When I eat out, I often adjust the tip to ensure that the total bill ends in “.00” or “.50”
This makes it easy to scan my credit card bill for false charges
 - Check your credit report using www.annualcreditreport.com.
Check a different one every 4 months
 - You can contact the 3 credit card agencies and have them put a fraud alert on your account.
 - Anyone trying to open an account in your name will be blocked and you will be asked to OK the transaction
 - You can get further information on Identity theft from the Federal Trade Commission <http://ftc.gov/idtheft>

What About Passwords?

- It is poor practice to use the same password for different sites
- How can I remember all these different passwords?
 - There is an App for that
 - I recommend LASTPASS (Free) <https://lastpass.com/>
 - Lastpass will remember and automatically fill out your login information
 - When you login to a site that's not in Lastpass data base ...
It will ask you if you want Lastpass to remember your login information
 - When you change the password at a site (and you should)
 - Lastpass will recognize what you are doing and offer to generate a password for you
 - It will then remember the new password for future logins
 - More information can be found in my Computer club handouts:
http://www.scscclb.club/smnr/Password_Managers.pdf

What else can I do?

- Some Cards (American Express) will send you a text alert anytime a payment is made and the card is not present.
 - You can also get alerts for purchases over a given amount
- Some Cards (Citi) will allow to get “Virtual Credit Cards”, which will expire on any date you specify.
 - You can also specify a maximum value for the card.
 - When making a purchase on a web site you are not familiar with
 - You can use a virtual card which expires the next day and is only good for the amount of the purchase.

What else can I do?

- Hackers often insert “skimmers” in the card slots of ATMs, Gas Pumps, etc.
 - If the card slot looks funny/different – check with the owner
 - To prevent them from “seeing” you enter your pin ...
Hold one hand over the keypad while you enter pin with the other
- Be alert when surfing the web
 - Consider adding Web of Trust to your browser
 - <https://www.mywot.com/>
 - This will add a circle next to links on the screen
 - Green = OK
 - Orange/Red = be careful/danger

Links/URL's

How to decipher a Link

- The secret is to locate the “Domain”
 - The domain consists of two parts, the domain name and the TLD/Country
 - The TLD is usually two to four letters, the Country Code is usually two letters
- For Example:
 - <https://abcd.efgh,ijkl.domain.xxx/mnop?qrst.uvw.xyz>
 - Do.not.reply@domain.xxx
- Typical TLD’s are:
 - *com, info, gov, net, edu, org, tv, and club*
 - Typical Country Code’s are:
 - *us* (USA), *ca* (Canada), *cn* (China), *jp* (Japan), and *ru* (Russia)

Known Phishing Sites

- Aetna.cm, aol.cm, chase.cm, citicards.cm, Costco.cm, facebook.cm, geico.cm, itunes.cm, suntrust.cm, turbotax.cm and Walmart.cm
- BofA.ch, Sears.tw,

Typical Links – Which are suspicious?

- <http://BofA.Accounts.cm/CustomerService>
- <http://BofA.Accounts.us/CustomerService>
- <http://donotreply.BofA.com/197835?google.com>
- notification+zrdpfzvzhrpz@facebookmail.com
- smith89134@cox.org
- registrar@unv.com
- SCSCS@yahoogroups.com
- support@amazon.jp
- reply@rs.email.nextdoor.com

Spam and Phishing

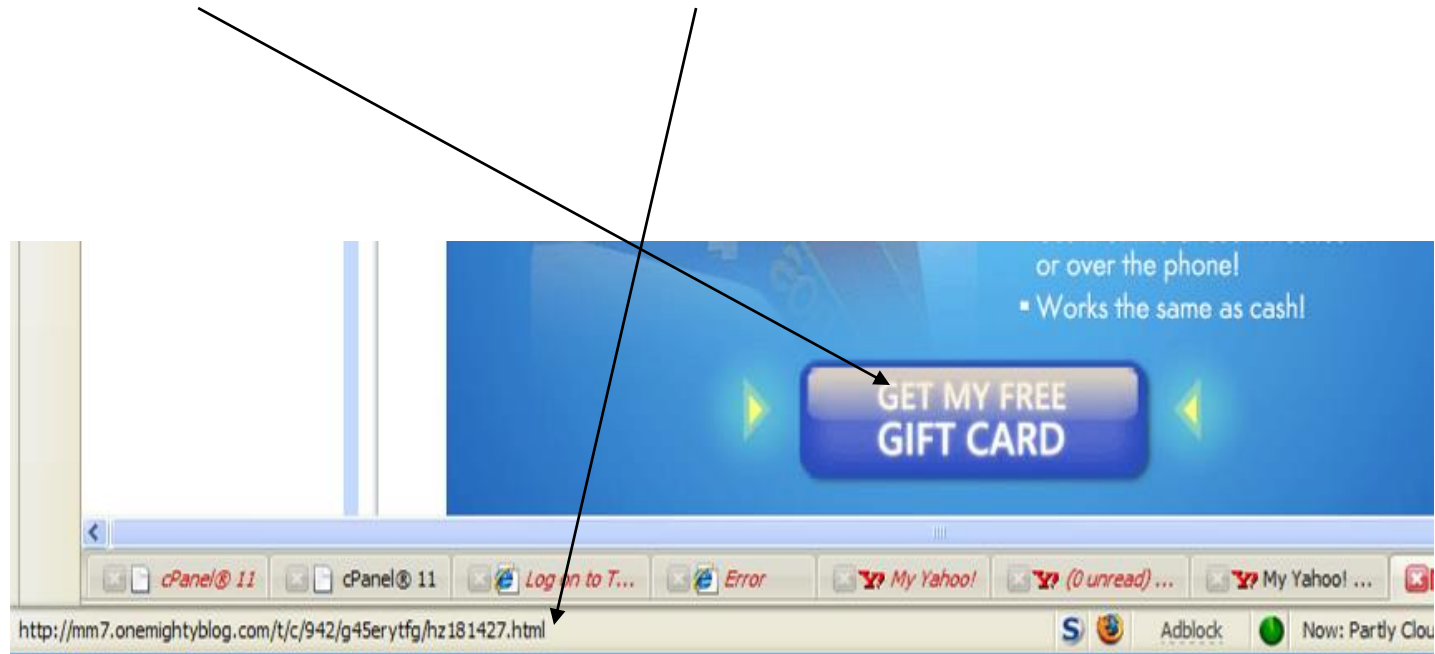
Phishing -1

- Phishing emails look like they came from a known source



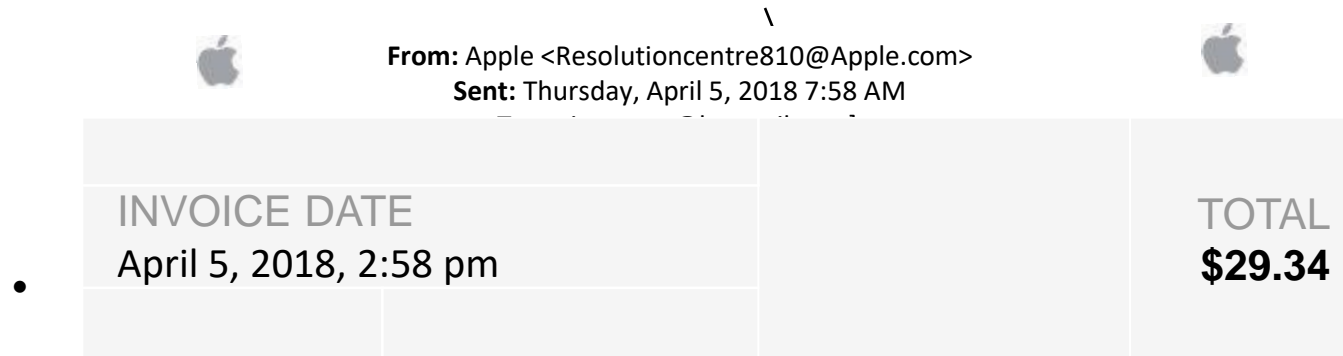
Phishing -2

- Check Links to see if they are what they say
 - Place Cursor over link, look at status bar



Phishing -3

- Check Links to see if they are what they are what they say
 - Place Cursor over link, look at status bar



- <https://mysp.ac/49C6n>

Phishing -4

- Good Practice is never click on links in suspicious mails
Instead, key the correct address into your browser's address bar
- If there are places in the email which ask you to key in personal info (SSN, Passwords, Account Numbers, etc.)
 - **DO NOT FILL THESE OUT!!**
- It is very easy to fake the *From* address – do NOT depend upon this to tell you who the sender is!

What else can I do?

- Do not trust links in email (even if from friends)
 - The “From” address, in email, is easy to fake
 - Your friend could be infected with a virus which uses his contact list to send copies of itself to everyone
 - Rather than just “clicking” on the link, type the address in the browser’s address bar directly
- Consider installing Web of Trust in your browser
 - WOT puts circles next to your links to indicate safety of site
 - <http://www.mywot.com>
- **BE PARANOID**

More Samples of Phishing

- Support <zIEYzYzrnoreply-zIEYzYzr@aryanot-nenek.com>

- Thu 2/22/2018, 1:00 PM

You added a new email address to your PayPal account
Dear, hverne@outlook.com

This is just a quick confirmation that you added a new email address (misterx531@yahoo.com) to your PayPal account.

If you want to make this your primary email address - where we'll send all your account-related information - log in to your PayPal account and go to your Profile.

If you didn't add this email, Please login to your account and ensure no one login to your account. It's important because it helps us make sure no one is getting into your account without your knowledge.

Is that you?

[Yes No, Secure My Account](#)

- Your action is required to help us to protect you PayPal account securely.
- Thank you. **PayPal.com**

More Samples of Phishing

From: Amazon FinalNotice <educationweek@edweek.org>

Sent: Saturday, August 26, 2017 2:32 PM

To:

Subject: Attn: Your Monthly Amazon Survey Statement Has Arrived
#1420134

[Final Notice : evie](#)

More Samples of Phishing

Costco Member Support <Costco_Member_Support@customer.ibonuscardsaving.us>

Sun 5/14/2017, 7:36 PM

Thank You for Being a Prime Member, \$50-Costco Card

=====
Costco Wholesale Member: ...

Account Ending in: 3897

Member Since: September 2015
=====

For a limited time only, We are awarding a \$50 Award to all Costco Members. You have been selected our of 1000s to take part in our anonymous survey about Costco Wholesale club.Go here to take our 30 second survey and redeem your \$50 gift to use at our wholesales clubs in the

US.: http://todayonly.ibonuscardsaving.us/intersection/22839881_costco

Thanks for choosing us,
Costco Wholesale

More Samples of Phishing

From: Walmart Notification <educationweek@ns1.astrocrown.eu>

Sent: Saturday, August 26, 2017 2:32 PM

To: ...

Subject: For our GREAT followers - Open Your Walmart Gift Box.

You've been chosen by Walmart to receive a \$50 reward!

—

**Get Your
\$50 Walmart Gift Card**



APPLY NOW

[Click Here to Get More Info](#)

Delete Facebook Account

https://www.facebook.com/help/delete_account?refid=69