Phishing

is the attempt to obtain sensitive information such as usernames, passwords, and credit card details (and sometimes,

indirectly, money), often for malicious

reasons, by masquerading as a trustworthy entity in an electronic communication. *(WiKi)*

General Knowledge about Internet Website Names and Phishing

1. Before checking name of any website, first look for the domain extension
i.e .com, .org, .co.in, .net, .in etc.
The name just before extension is the DOMAIN NAME of the website.
Eg: www.domainname.com

E.g., in http://amazon.diwali-festivals.com, the word before .com is "diwali-festivals" (and NOT "amazon").
AMAZON word is seperated with (.) dot So, this webpage does not belong to amazon.com, but it belongs to "diwali-festivals.com", which most of us haven't heard of before.

You can similarly check for fraudulent (so-called) banking websites.
Before your e-banking login, make sure that the name just before ".com" is the name of your bank.

Eg:
"something.icicibank.com" belongs to +ICICI*,
but "icicibank.something.com" belongs to something and not icicibank.
"icicibank.com.nu" belongs to "com"!

2. There can also be a typo in domain done purposly to confuse user to do phishing. Eg: www.facebookk.com or faceb(00)k.com does not relates to facebook.com

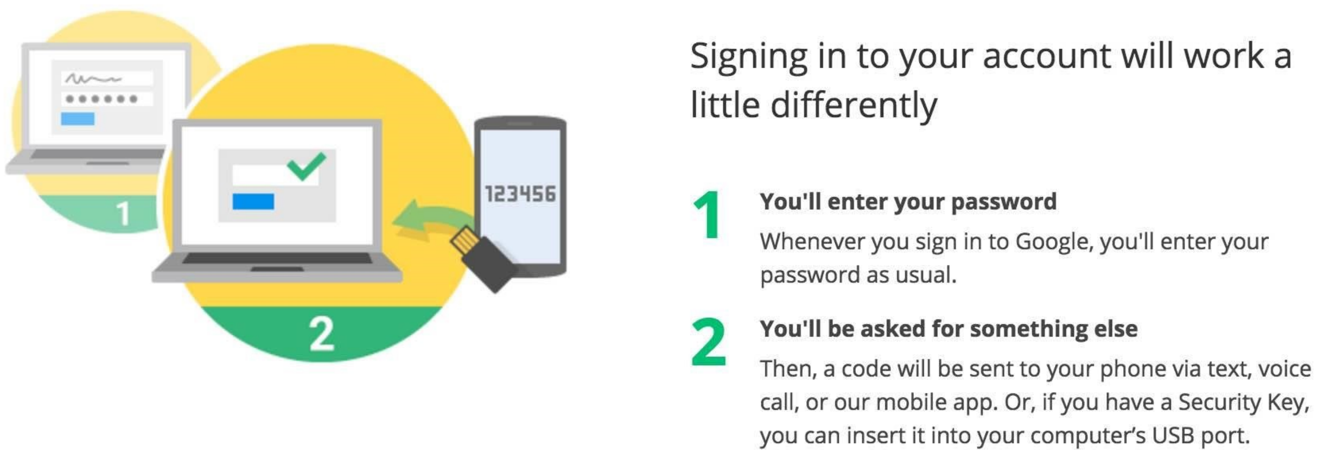
3. Nowdays you may have also seen various spam messages forwarded by users claiming to get free mobile or mobile phone at Rs.250/- or Free Talktime etc.

Before attempting to forward such messages, always check for domain name and website. Inputing data and doing some task as said on their website may result in your smartphone infected by some malware. There are several scripts present on such website which may be executed. So Beware and dont fall in such trap. There is nothing FREE in this world.

4. Also please check before downloading apk or android apps for smartphone. http://googleplay.com/store/apps/com.ife.google
Does not belongs to Google, it belongs to googleplay.com which is not owned by Google.
But http://play.google.com/store/apps/com.ife.google belongs to Google.

Please share this information widely and help your family and friends avoid falling for such tricks.

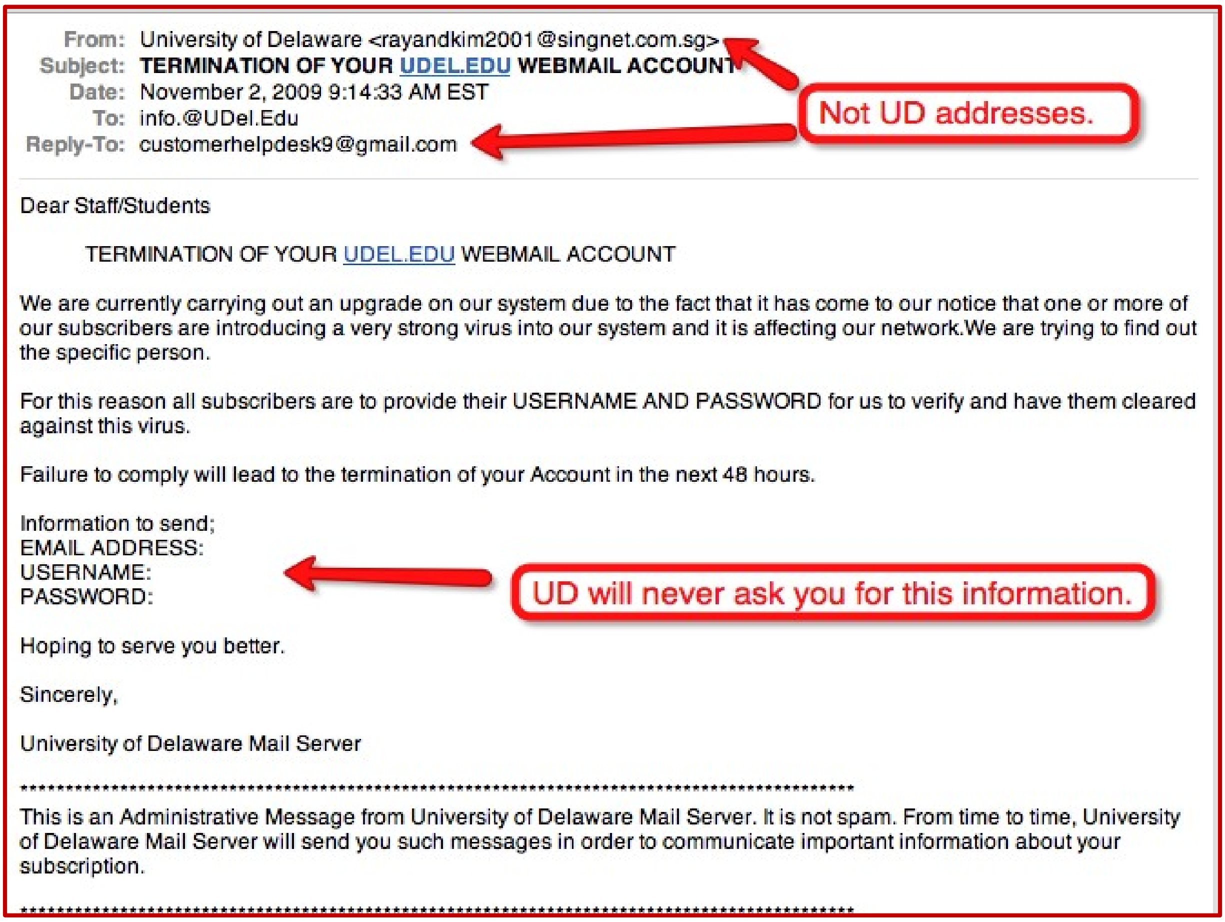
SOME EXAMPLES



Signing in to your account will work a little differently

1 **You'll enter your password**
Whenever you sign in to Google, you'll enter your password as usual.

2 **You'll be asked for something else**
Then, a code will be sent to your phone via text, voice call, or our mobile app. Or, if you have a Security Key, you can insert it into your computer's USB port.



From: University of Delaware <rayandkim2001@singnet.com.sg>
Subject: **TERMINATION OF YOUR UDEL.EDU WEBMAIL ACCOUNT**
Date: November 2, 2009 9:14:33 AM EST
To: info.@UDel.Edu
Reply-To: customerhelpdesk9@gmail.com

Not UD addresses.

Dear Staff/Students

TERMINATION OF YOUR UDEL.EDU WEBMAIL ACCOUNT

We are currently carrying out an upgrade on our system due to the fact that it has come to our notice that one or more of our subscribers are introducing a very strong virus into our system and it is affecting our network.We are trying to find out the specific person.

For this reason all subscribers are to provide their USERNAME AND PASSWORD for us to verify and have them cleared against this virus.

Failure to comply will lead to the termination of your Account in the next 48 hours.

Information to send;
EMAIL ADDRESS:
USERNAME:
PASSWORD:

UD will never ask you for this information.

Hoping to serve you better.

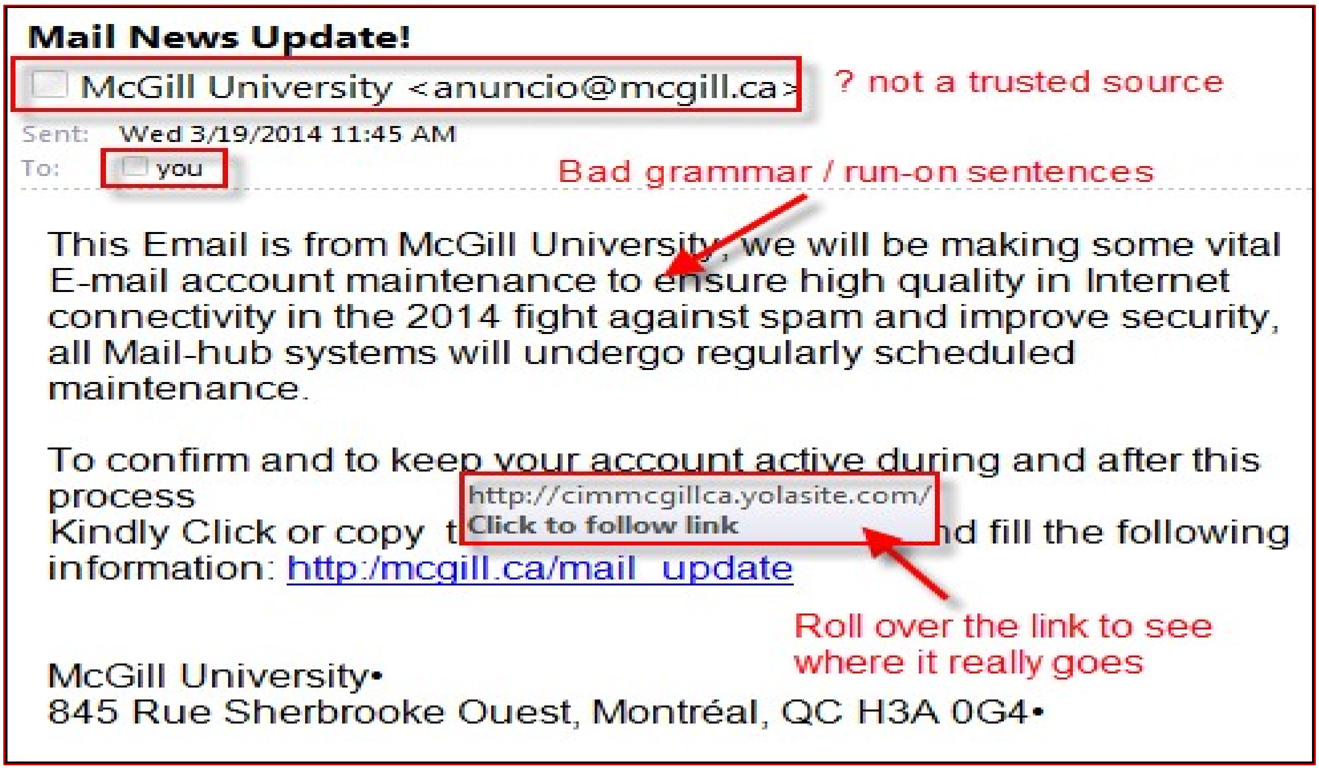
Sincerely,

University of Delaware Mail Server

****

This is an Administrative Message from University of Delaware Mail Server. It is not spam. From time to time, University of Delaware Mail Server will send you such messages in order to communicate important information about your subscription.

****



Mail News Update!

McGill University <anuncio@mcgill.ca>

Sent: Wed 3/19/2014 11:45 AM

To: you

This Email is from McGill University, we will be making some vital E-mail account maintenance to ensure high quality in Internet connectivity in the 2014 fight against spam and improve security, all Mail-hub systems will undergo regularly scheduled maintenance.

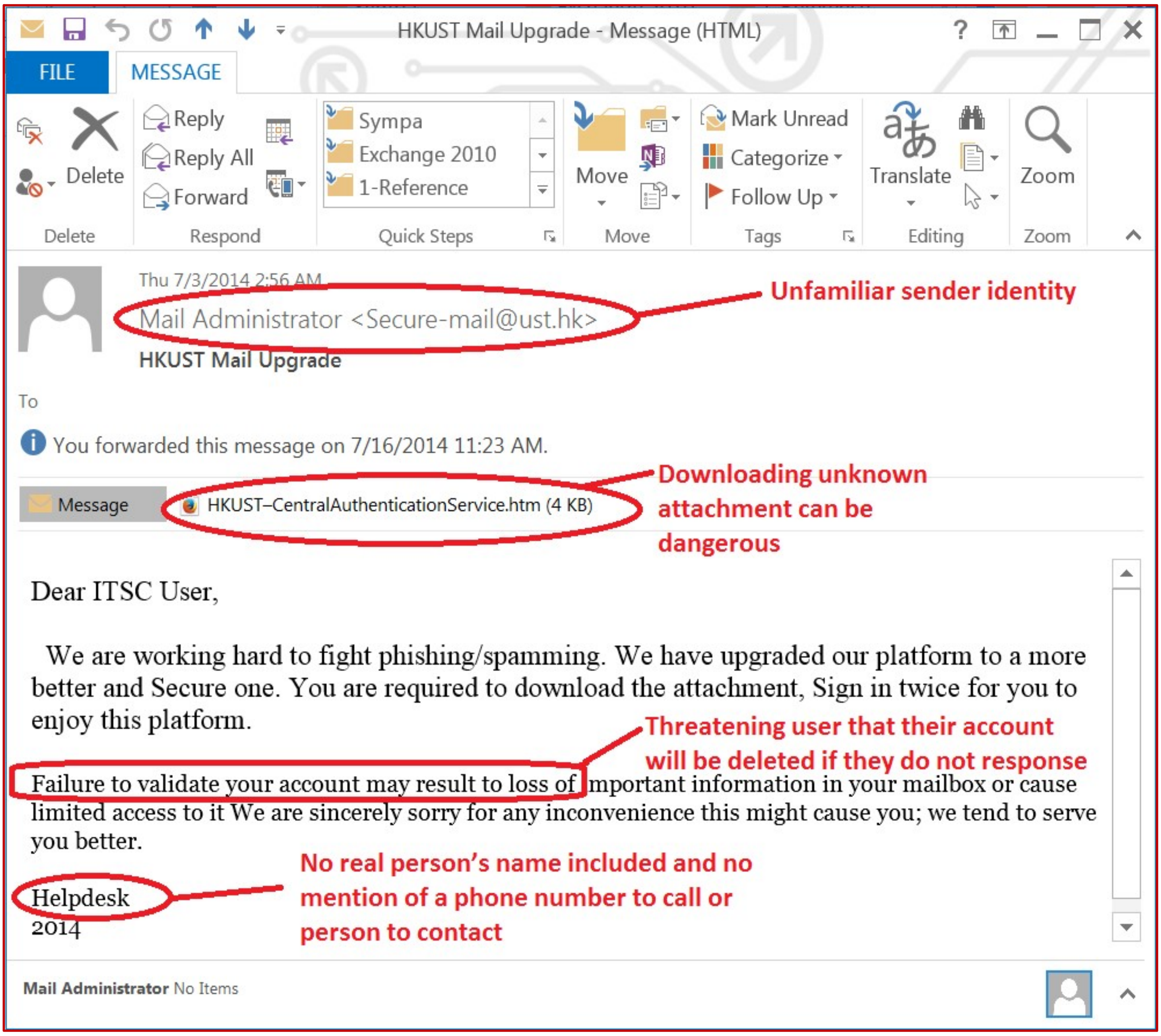
To confirm and to keep your account active during and after this process
Kindly Click or copy t[http://cimmcgillca.yolasite.com/ Click to follow link]nd fill the following information: http:/mcgill.ca/mail_update

McGill University•
845 Rue Sherbrooke Ouest, Montréal, QC H3A 0G4•

? not a trusted source

Bad grammar / run-on sentences

Roll over the link to see where it really goes



Thu 7/3/2014 2:56 AM

Mail Administrator <Secure-mail@ust.hk>

HKUST Mail Upgrade

To

You forwarded this message on 7/16/2014 11:23 AM.

Message | HKUST–CentralAuthenticationService.htm (4 KB)

Dear ITSC User,

We are working hard to fight phishing/spamming. We have upgraded our platform to a more better and Secure one. You are required to download the attachment, Sign in twice for you to enjoy this platform.

Failure to validate your account may result to loss of important information in your mailbox or cause limited access to it We are sincerely sorry for any inconvenience this might cause you; we tend to serve you better.

Helpdesk
2014

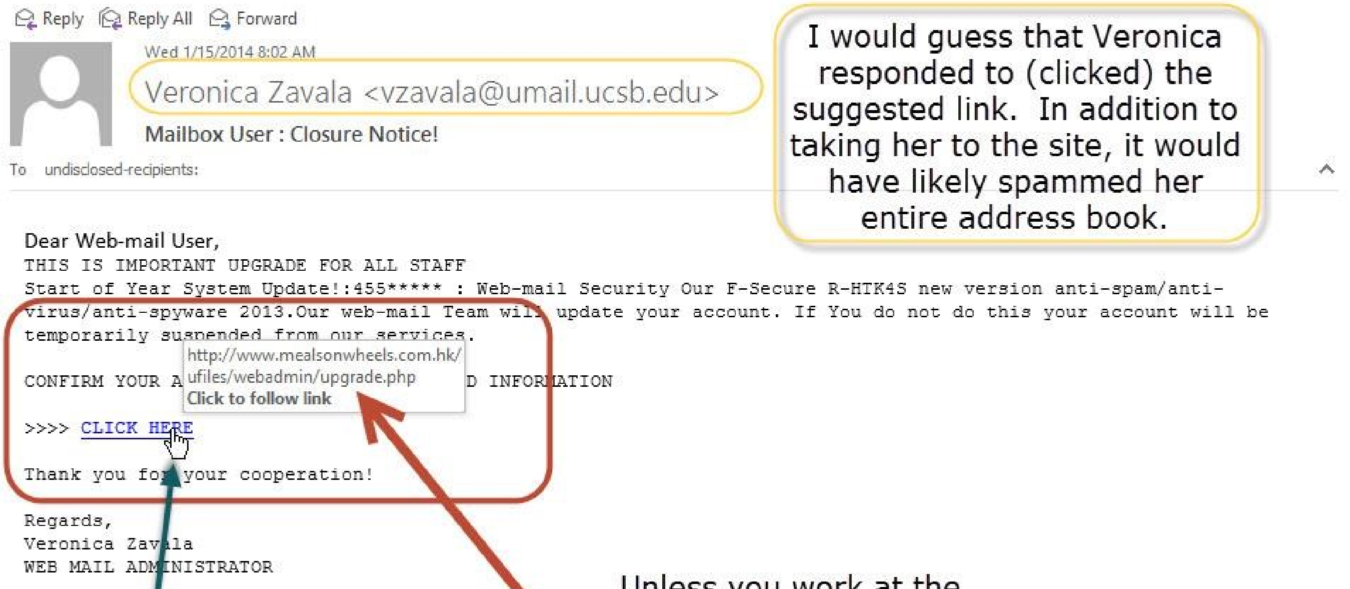
Mail Administrator No Items

Unfamiliar sender identity

Downloading unknown attachment can be dangerous

Threatening user that their account will be deleted if they do not response

No real person's name included and no mention of a phone number to call or person to contact



Wed 1/15/2014 8:02 AM

Veronica Zavala <vzavala@umail.ucsb.edu>

Mailbox User : Closure Notice!

To undisclosed-recipients:

Dear Web-mail User,
THIS IS IMPORTANT UPGRADE FOR ALL STAFF
Start of Year System Update!:455***** : Web-mail Security Our F-Secure R-HTK4S new version anti-spam/anti-virus/anti-spyware 2013.Our web-mail Team will update your account. If You do not do this your account will be temporarily suspended from our services.

CONFIRM YOUR A D INFORMATION

http://www.mealsonwheels.com.hk/ufiles/webadmin/upgrade.php
Click to follow link

>>>> CLICK HERE

Thank you for your cooperation!

Regards,
Veronica Zavala
WEB MAIL ADMINISTRATOR

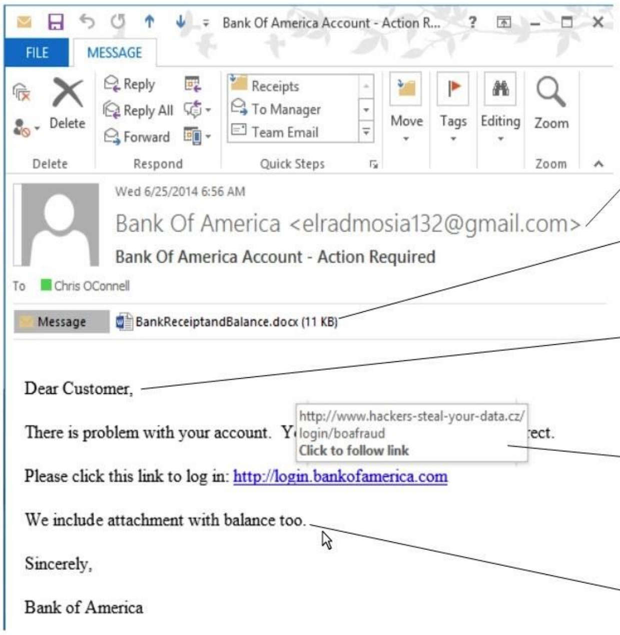
I would guess that Veronica responded to (clicked) the suggested link. In addition to taking her to the site, it would have likely spammed her entire address book.

Unless you work at the Hongkong (.hk) branch of "Meals on Wheels" this would likely be a phishing attempt.

Hover the mouse point over the suggested link WITHOUT CLICKING to reveal the true destination you would be sent to.

Note: on our webmail, the revealed link would appear on the bottom left of the window.

5 Ways to be ***SAFE*** from Malicious Emails



Wed 6/25/2014 6:56 AM

Bank Of America <elradmosia132@gmail.com>

Bank Of America Account - Action Required

To Chris OConnell

Message BankReceiptandBalance.docx (11 KB)

Dear Customer,

There is problem with your account. Y ect.

http://www.hackers-steal-your-data.cz/login/boafraud
Click to follow link

Please click this link to log in: http://login.bankofamerica.com

We include attachment with balance too.

Sincerely,

Bank of America

Email says it's coming from a company, but is actually from a personal email service.

Never open attachments unless you're 100% sure they are from a trusted source.

Be wary of generically addressed emails!

Hover over a link without clicking. This shows where the link will actually take you. **If you don't recognize the site don't click!**

Grammatical or spelling errors indicate a fake!

What to do: If you are even 1% uncertain about this email flag it as junk. NEVER FORWARD TO COWORKERS (unless it's your IT person). You can forward it to your IT person if you need confirmation that the email is fake.

10 Tips to Prevent Phishing Attacks:

1. Learn to Identify Suspected Phishing Emails

There are some qualities that identify an attack through an email:

- They duplicate the image of a real company.
- Copy the name of a company or an actual employee of the company.
- Include sites that are visually similar to a real business.
- Promote gifts, or the loss of an existing account.

2. Check the Source of Information from Incoming Mail

Your bank will never ask you to send your passwords or personal information by mail. Never respond to these questions, and if you have the slightest doubt, call your bank directly for clarification.

3. Never Go to Your Bank’s Website by Clicking on Links Included in Emails

Do not click on hyperlinks or links attached in the email, as it might direct you to a fraudulent website.

Type in the URL directly into your browser or use bookmarks / favorites if you want to go faster.

4. Enhance the Security of Your Computer

Common sense and good judgment is as vital as keeping your computer protected with a good antivirus to block this type of attack.

In addition, you should always have the most recent update on your operating system and web browsers.

5. Enter Your Sensitive Data in Secure Websites Only

In order for a site to be ‘safe’, it must begin with ‘https://’ and your browser should show an icon of a closed lock.

6. Periodically Check Your Accounts

It never hurts to check your bank accounts periodically to be aware of any irregularities in your online transactions.

7. Phishing Doesn’t Only Pertain to Online Banking

Most phishing attacks are against banks, but can also use any popular website to steal personal data such as eBay, Facebook, PayPal, etc.

8. Phishing Knows All Languages

Phishing knows no boundaries, and can reach you in any language. In general, they’re poorly written or translated, so this may be another indicator that something is wrong.

If you never you go to the Spanish website of your bank, why should your statements now be in this language?

9. Have the Slightest Doubt, Do Not Risk It

The best way to prevent phishing is to consistently reject any email or news that asks you to provide confidential data.

Delete these emails and call your bank to clarify any doubts.

10. Check Back Frequently to Read About the Evolution of Malware

If you want to keep up to date with the latest malware attacks, recommendations or advice to avoid any danger on the net, etc …

you can always read our blog or follow us on Twitter and Facebook

Happy to answer any questions you may have!

- www.Facebook.com/Anir0y
- Twitter @anr0y