Special Olympics Ireland

Cyber Awareness Training

DELLEMC

Be Cyber AWARE

Welcome ☺

Quick questions

Show of hands….

- Who has a smart phone,
- Who has a Facebook account,
- Who has an Instagram account,
- Who shares photos with others and regularly posts with others.

Wow!

- It’s great to see so many people with phones and social media accounts.
- We hope that with today’s session that we will help make you more **Cyber Aware** and help you to be **Cyber Safe**

Shout out - what these words mean….

AWARE

What is Cyber Aware?

Definition of ***cyber*** in English:
ADJECTIVE

Anything to do with computers, information technology, and virtual reality.

Origin: Abbreviation of cybernetics.

Definition of ***aware*** in English:
ADJECTIVE*(with adverb or in combination)*

Concerned and well informed.

© Oxford English Dictionary

Cyber Space Your Digital Footprint

Cyber Space: Your Digital Footprint

Cyber Aware

Did you know that everytime you go online you leave a trail which will never be erased?

Nothing is truly private on the internet.

Cyber Aware

Cyber Space: Your Digital Footprint

Your digital footprint is what's left behind as you casually browse the web, post on social media or even type into a chat service.

The digital footprint can have unexpected effects in all areas of your life, potentially resulting in:

- public sharing of personal information
- putting yourself in unintended danger
- Relationships

Today we will talk about being more aware of how you manage yourself and your online activity

Your digital footprint is 100% within your control
Be Cyber Aware – Be Safe

Tips for Securing your Social Media –

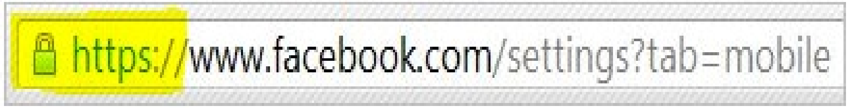
Using Facebook

Hackers, fraudsters, identity thieves and others all use and hack into Facebook profiles as a means to their illegal ends. So, what exactly are the best ways to keep your Facebook account safe and secure?

1. Manage Your Security Settings

- The above picture will allow you to modify settings regarding your security questions, app passwords, current active sessions, and more. Checking, and enabling all of these options and features will improve the security around your Facebook account.

2. Use a Secure Browsing



https://www.facebook.com/settings?tab=mobile

- A HTTP secure connection is achieved whenever the URL begins with https:// instead of http://

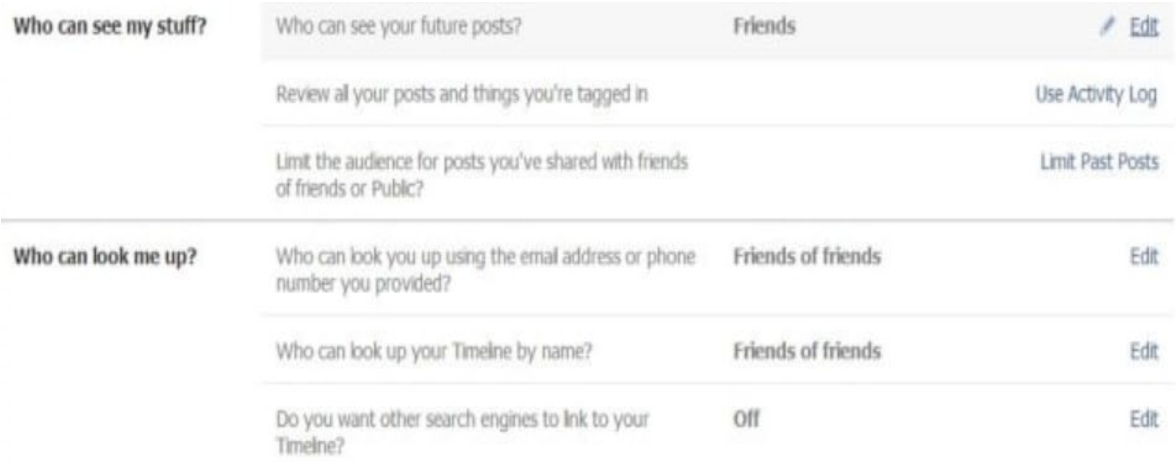
- Browsing Facebook without an HTTP secure connection keeps your data open to attacks any time you use free Wi-Fi (for example using free Wi-Fi in Starbucks, a public library or a hotel)

3. Only Add Real Friends

- Many Facebook users are unaware of the dangers of accepting random friend requests. Becoming friends with somebody on Facebook allows them to access personal information about you, including your full name, location, place of birth, birthday and more.

- This information can easily be exploited by identity thieves, and so it’s always the best policy to reject friend requests from people you don’t actually know in person.

4. Customize Your Facebook Privacy Settings



Who can see my stuff?	Who can see your future posts?	Friends	Edit
	Review all your posts and things you're tagged in		Use Activity Log
	Limit the audience for posts you've shared with friends of friends or Public?		Limit Past Posts
Who can look me up?	Who can look you up using the email address or phone number you provided?	Friends of friends	Edit
	Who can look up your Timeline by name?	Friends of friends	Edit
	Do you want other search engines to link to your Timeline?	Off	Edit

- Keeping your personal information private, is a great idea in terms of security. By default, information such as your date of birth, location, etc are all accessible to Facebook users who do not know you.

- To change this, go into your privacy settings, which can be found by clicking on the gear button located at the top right-hand corner of your Facebook screen, followed by clicking **"Privacy Settings"**.

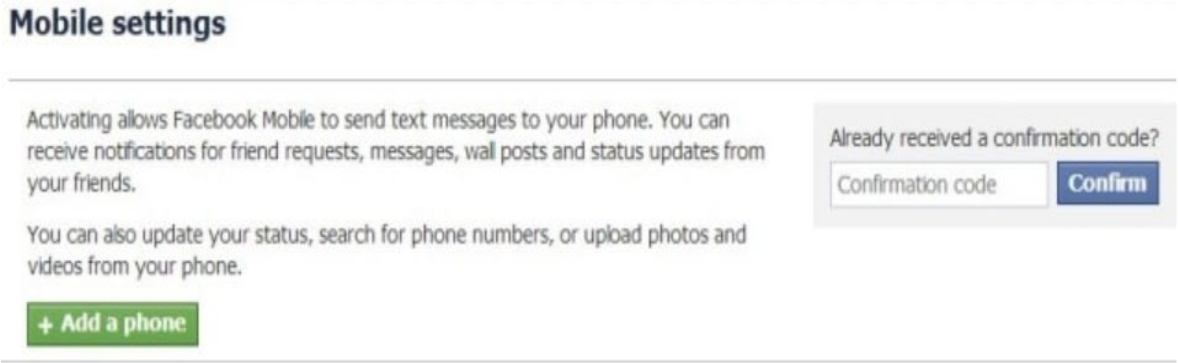
5. Don’t Overuse Passwords

- Using the same password for your email address and your Facebook account is asking for big, big trouble.
- A hacker who gains access to your Facebook account will immediately have access to your registered email address. Using the same password for both accounts allows them to be able to get information, files, images, passwords, and more. So, it is hugely important to take the time to create separate passwords for each of your accounts.

6. Log Out After You Use Facebook

- If you are browsing the web on public devices such as at libraries, forgetting to log out of your Facebook account can prove very dangerous
- Although you may be lucky to get away with a prank, there is a risk of becoming a victim of fraud, identity theft, or worse.

7. Confirm Your Mobile Number



Mobile settings

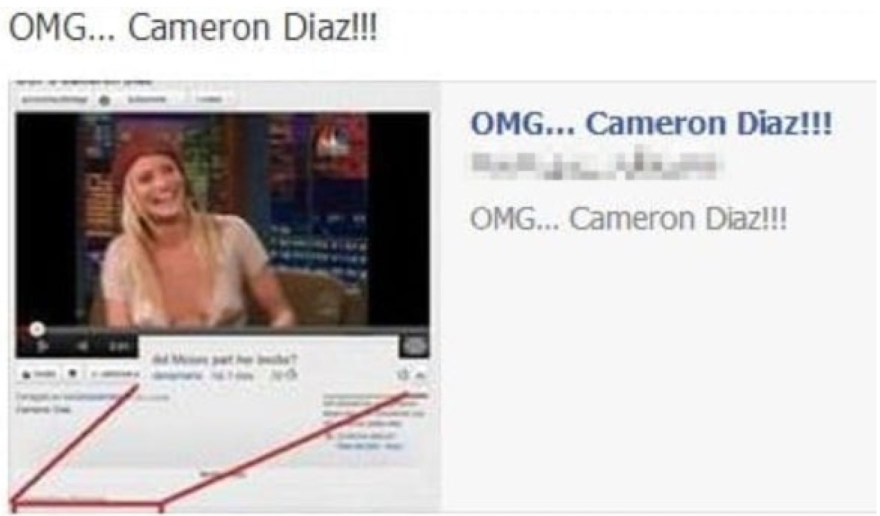
Activating allows Facebook Mobile to send text messages to your phone. You can receive notifications for friend requests, messages, wall posts and status updates from your friends.

You can also update your status, search for phone numbers, or upload photos and videos from your phone.

- Along with adding trusted contacts, confirming your mobile number is one of many ways to imporve your account security on Facebook. This way, even when you lose or forget your password, Facebook will be able to send you a new one via SMS.

- To access this option, click on the gear button located at the top right-hand corner of your Facebook screen, followed by clicking **“Account Settings”**, then by clicking **“Mobile”** on the left-hand sidebar.

8. Avoid Spam Links



OMG... Cameron Diaz!!!

OMG... Cameron Diaz!!!

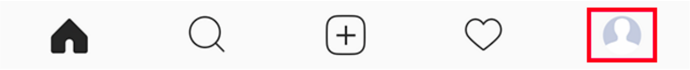
OMG... Cameron Diaz!!!

- There are more and more spam links appearing on Facebook feeds of every user. An example of link attacks include money scams through direct or indirect requests via Facebook messages. Phishing links that will redirect you to fake websites are also showing up more regularly on Facebook feeds.
- These malicious links are able to get your personal information or even harm your computer. There are also chances you may receive emails from 'Facebook' – when in reality, a phishing website is trying to trick you into a scam, or worse.

9. Use A Strong Password

- Strong passwords are essential for all online and offline applications, but Facebook especially. with over 600,000 Facebook hackings every day, having an unusual password might be a good idea. Adding a mixture of numbers, letters and a special character, along with upper and lower case letters.

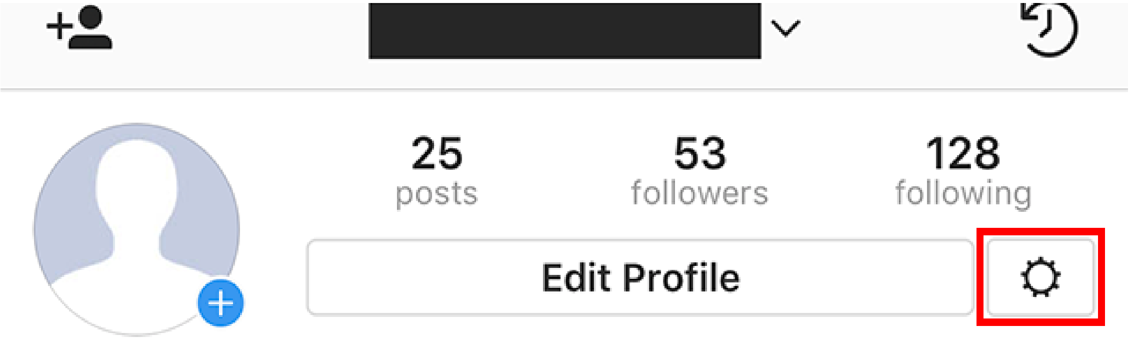
Using Instagram



1: Turn Your Instagram Page on Private

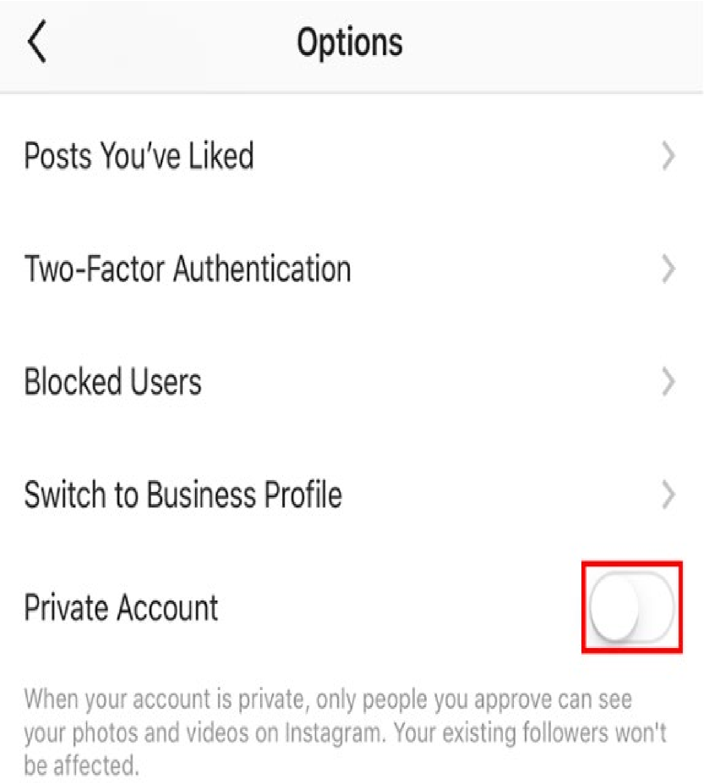
Step 1 : Tap your profile picture in the bottom-right corner of the screen.

Step 2: Tap the gear icon near the top-right corner of the screen.


[redacted]

DELLEMC

Step 3: Scroll down and tap the toggle next to “Private Account” to make your account private. The toggle will turn blue.



Options

Posts You’ve Liked

Two-Factor Authentication

Blocked Users

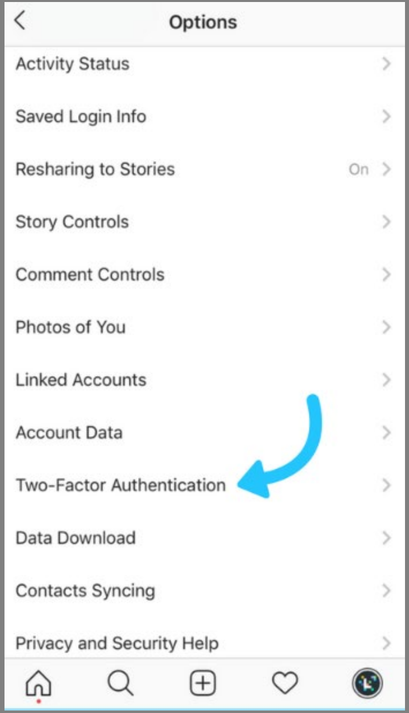
Switch to Business Profile

Private Account

When your account is private, only people you approve can see your photos and videos on Instagram. Your existing followers won't be affected.

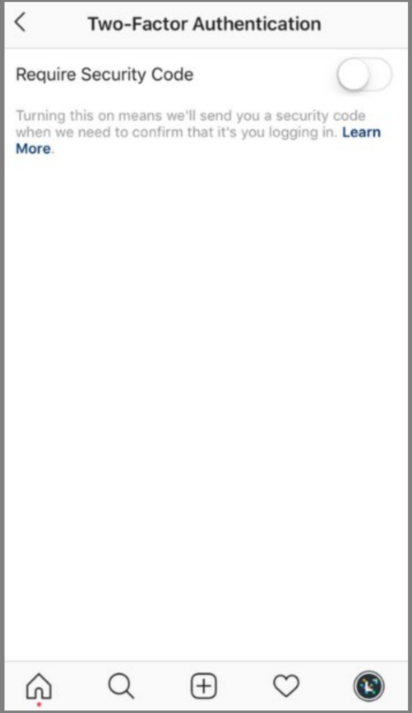
2: Turn on Two-Factor Authentication

- Most major social media platforms now provide some form of two-factor authentication and this includes Instagram.
- With two-factor authentication turned on, whenever you log into Instagram from an unrecognized device, you’ll be asked to enter an SMS security code, along with your username and password. This can help stop any attempts by hackers to log into your account and change your contact information.
- To turn two-factor authentication on, head to your Instagram profile and tap the settings button. Then scroll down and tap Two-Factor Authentication.



Options

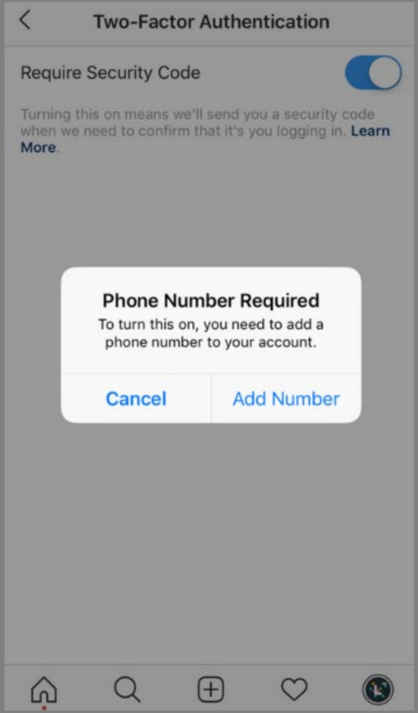
- Activity Status
- Saved Login Info
- Resharing to Stories On
- Story Controls
- Comment Controls
- Photos of You
- Linked Accounts
- Account Data
- Two-Factor Authentication
- Data Download
- Contacts Syncing
- Privacy and Security Help



Two-Factor Authentication

Require Security Code

Turning this on means we'll send you a security code when we need to confirm that it's you logging in. Learn More.



Two-Factor Authentication

Require Security Code

Turning this on means we'll send you a security code when we need to confirm that it's you logging in. Learn More.

Phone Number Required

To turn this on, you need to add a phone number to your account.

Cancel | Add Number

How to Turn on Two Factor Authentication

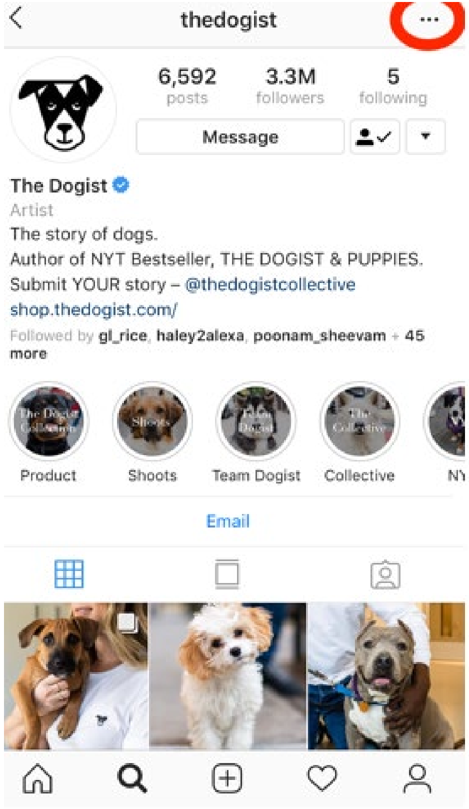
3. Block Unknown or Harassing Followers

- Instagram doesn’t offer a way to protect users from receiving anonymous messages. you can block followers and people who send inappropriate direct messages.

KEEP PERSONAL DETAILS PRIVATE
BLOCK UNKNOWN OR HARASSING FOLLOWERS
REMOVE PHOTO TAGS
DELETE PHOTOS
REVOKE ACCESS BY THIRD-PARTY APPS

How to Block Users

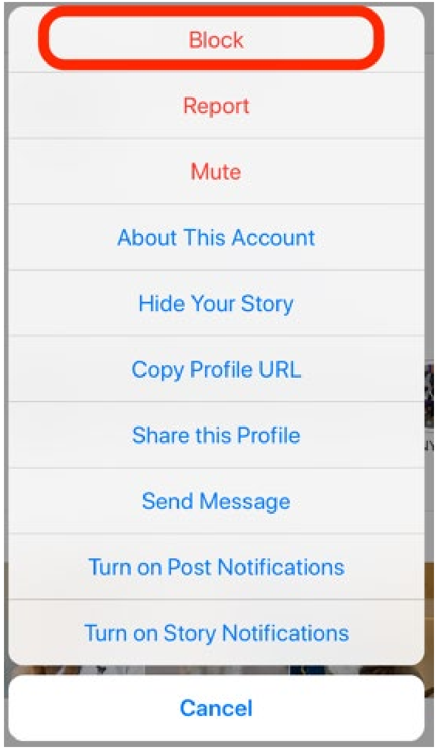
- From your list of **Followers** (or in the **direct message folder**), tap through to the profile of the user you wish to block.
- Tap the **three dots** in the top-right corner.



The Dogist
Artist
The story of dogs.
Author of NYT Bestseller, THE DOGIST & PUPPIES.
Submit YOUR story – @thedogistcollective
shop.thedogist.com/
Followed by gl_rice, haley2alexa, poonam_sheevam + 45 more

How to Block Users

- Tap **Block**.
- You can block anyone — even people who aren't followers. What's more, blocked users don't know that they've been blocked. If you block someone accidentally, just follow the steps above to unblock them again.



Tea Break

Back in 15 minutes

Using Snapchat

Private Info Sharing

Private Info Sharing
World Wide Web Rule

W –Who is asking for your personal information?

W –What information is being requested?

W – Why do they need your personal information?

WWW Rule – Sharing Personal Information

- Take care with giving out personal information. It may be used against you
  - to steal money from you or to download malware on your machine.
- Banks would never ask you for your personal bank details.
- Companies would contact ring you asking you for private information.

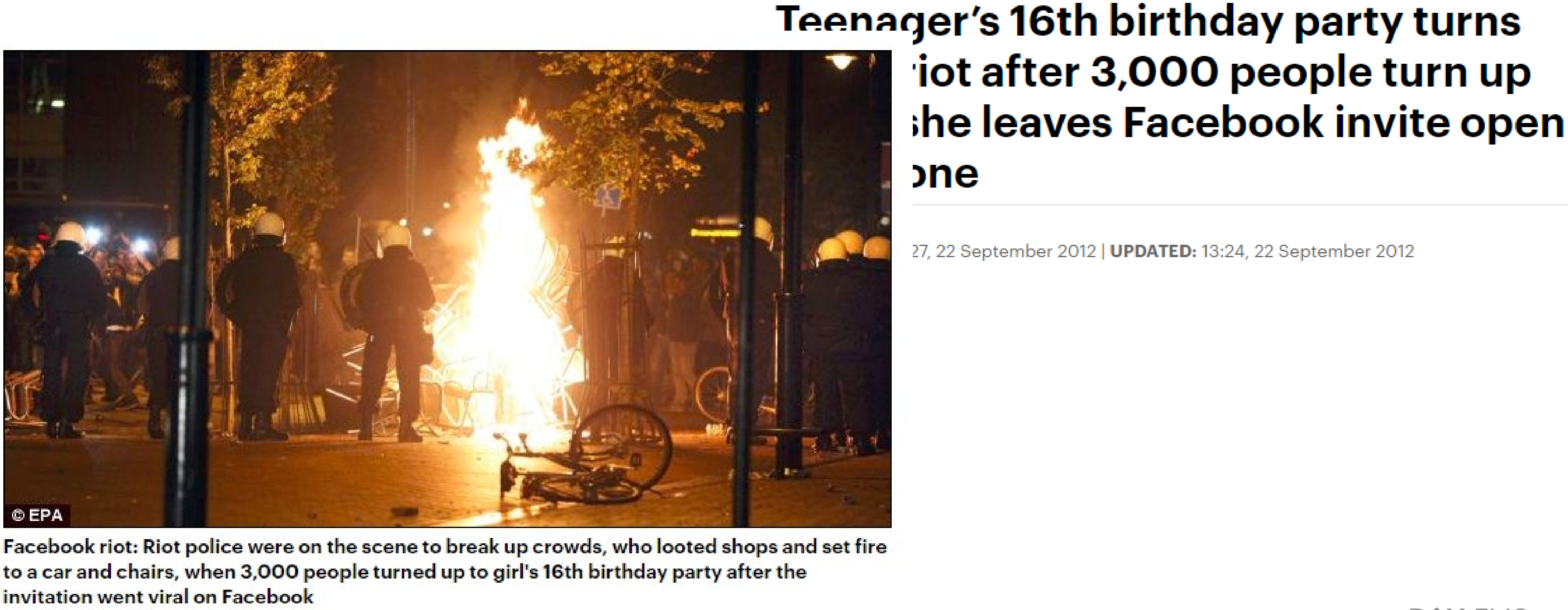
Cyber Aware

- If something or someone online makes you feel uncomfortable, **you have the right to not respond, delete a post, and most importantly tell a trusted adult/carer.**

- Never meet in person with anyone you've only met online.

- Never use the Internet to spread gossip, bully or hurt someone's reputation.

Organising a Party?
Don’t post it on social media



Teenager’s 16th birthday party turns riot after 3,000 people turn up she leaves Facebook invite open one

27, 22 September 2012 | **UPDATED:** 13:24, 22 September 2012

© EPA

Facebook riot: Riot police were on the scene to break up crowds, who looted shops and set fire to a car and chairs, when 3,000 people turned up to girl's 16th birthday party after the invitation went viral on Facebook

Telling your Friends you are on Holiday?

- Posting holiday pictures or posting travel details could tell burglars your house will be empty!!

- *Get Safe Online, a UK government-backed organisation that gives guidance on how to stay safe while using the internet, said: “It’s great posting updates or pics about what a fantastic holiday you’re having, but that could also be telling everyone that your home is unoccupied. Think before you post or send.”*

Posting holiday pictures on social media while abroad is increasingly common CREDIT: GETTY

Free Clip Art ...

DELLEMC

Password Aware

Cyber Key

Hackers can use your password to gain access to ALL your personal accounts

Make your password stronger with four random words

simply amazing quantum fog

Choose words that are memorable but avoid those which might be easy to guess, such as 'onetwothree' or are closely related to you personally, such as the names of family members or pets.

Cyber Key

Cyber Aware

Make your password stronger with four random words

simplyamazingquantumfog

It would take a computer about
277 TRILLION YEARS
to crack your password

Cyber Key

Make your password stronger with four random words

Simply Amazing Quantum Fog

It would take a computer about
1 NONILLION YEARS
to crack your password

Cyber Key

Make your password stronger with four random words

Simply Amazing Quantum Fog

It would take a computer about
1 NONILLION YEARS
to crack your password

1,000,000,000,000,000,000,000,000,000,000 years

Good or Bad Password Game

Good Password/Bad Password Game

Password

Good Password/Bad Password Game

Good Password/Bad Password Game

RuthKelly

Good Password/Bad Password Game

Rut[illegible]lly

Good Password/Bad Password Game

Sunshine Iceberg Cable Table

Good Password/Bad Password Game

Sunshine Iceberg Cable Table

✓

Good Password/Bad Password Game

12345

Good Password/Bad Password Game

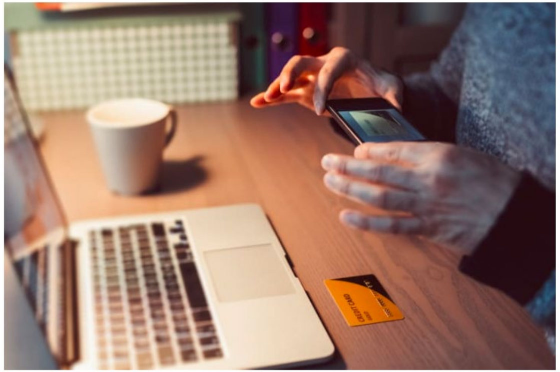
123

Cyber Sharing - Photos

Sharing Photo Awareness

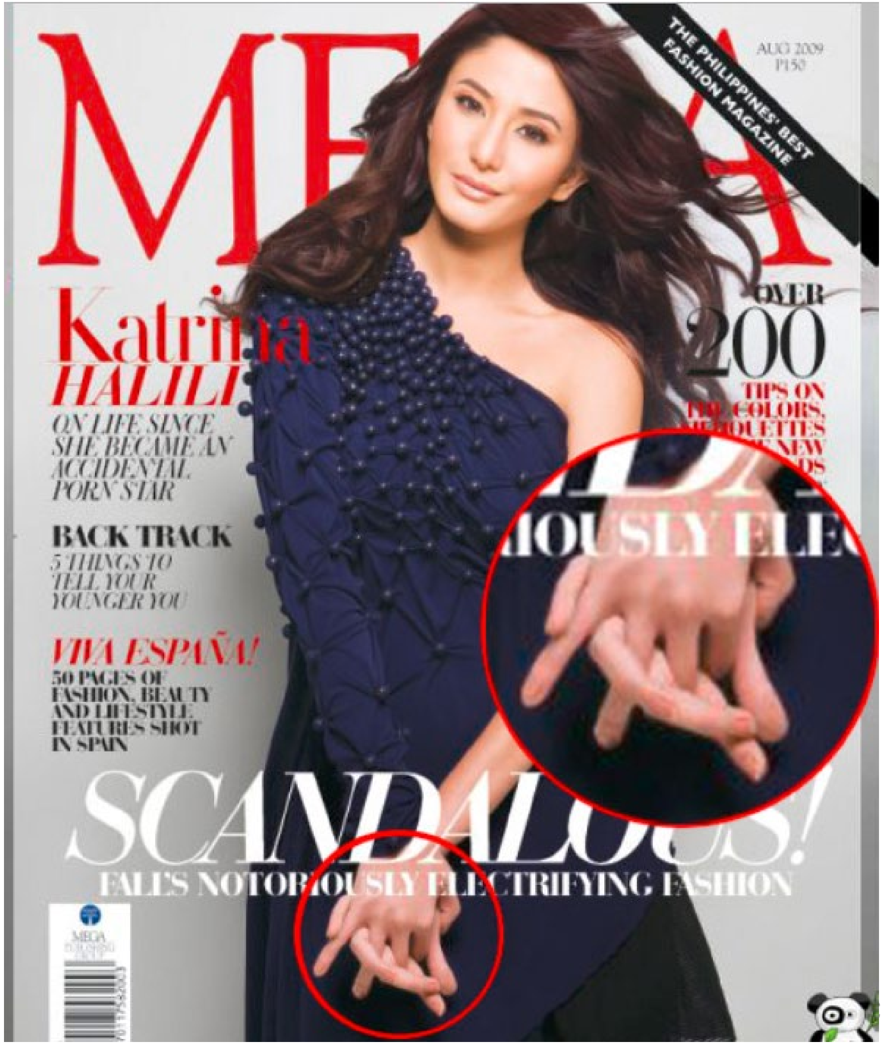
- Don’t post photos of other people, people’s children on Social Media if you do not have their permission.
- Do not give away personal information on your photos
  - For example address info
  - Bank information

iStock

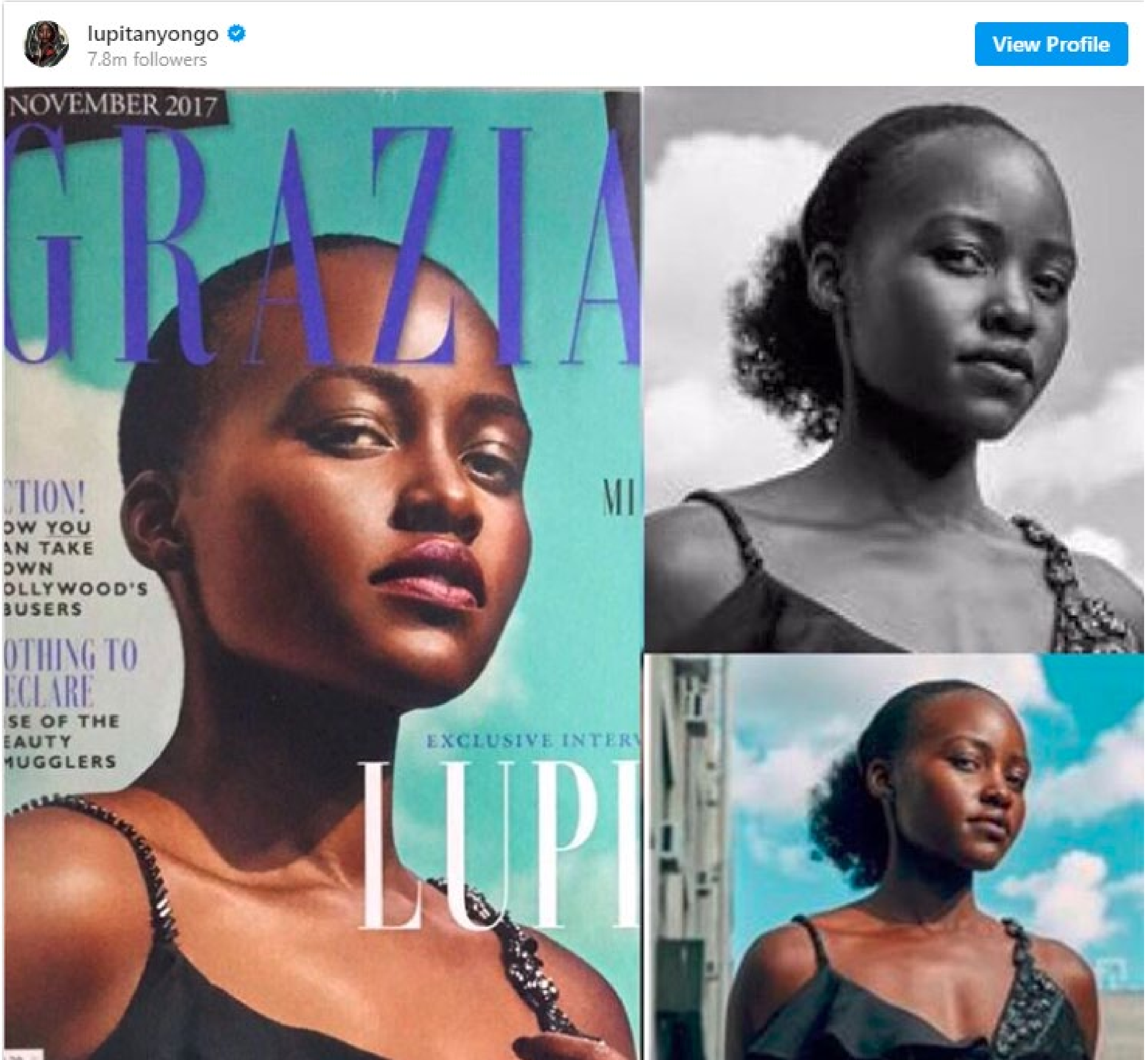


iStock

Have Fun with Photos – BUT note when its sent it is no longer in your control


MEGA
THE PHILIPPINES' BEST FASHION MAGAZINE
AUG 2009
P150
Katrina
HALILI
ON LIFE SINCE SHE BECAME AN ACCIDENTAL PORN STAR
BACK TRACK
5 THINGS TO TELL YOUR YOUNGER YOU
VIVA ESPAÑA!
50 PAGES OF FASHION, BEAUTY AND LIFESTYLE FEATURES SHOT IN SPAIN
OVER
200
TIPS ON
THE COLORS,
SILHOUETTES
NEW
DS
SCANDALOUS!
FALL'S NOTORIOUSLY ELECTRIFYING FASHION
MEGA

boredpanda.com



lupitanyongo

7.8m followers

We get it, Incredible BULK (Source Daily Doze YouTube)

Cyber Sharing

There are 3.2 billion people online.
You don’t have to share with all of them

Remember post only what you would feel comfortable with your family, your mentor and the whole world seeing.

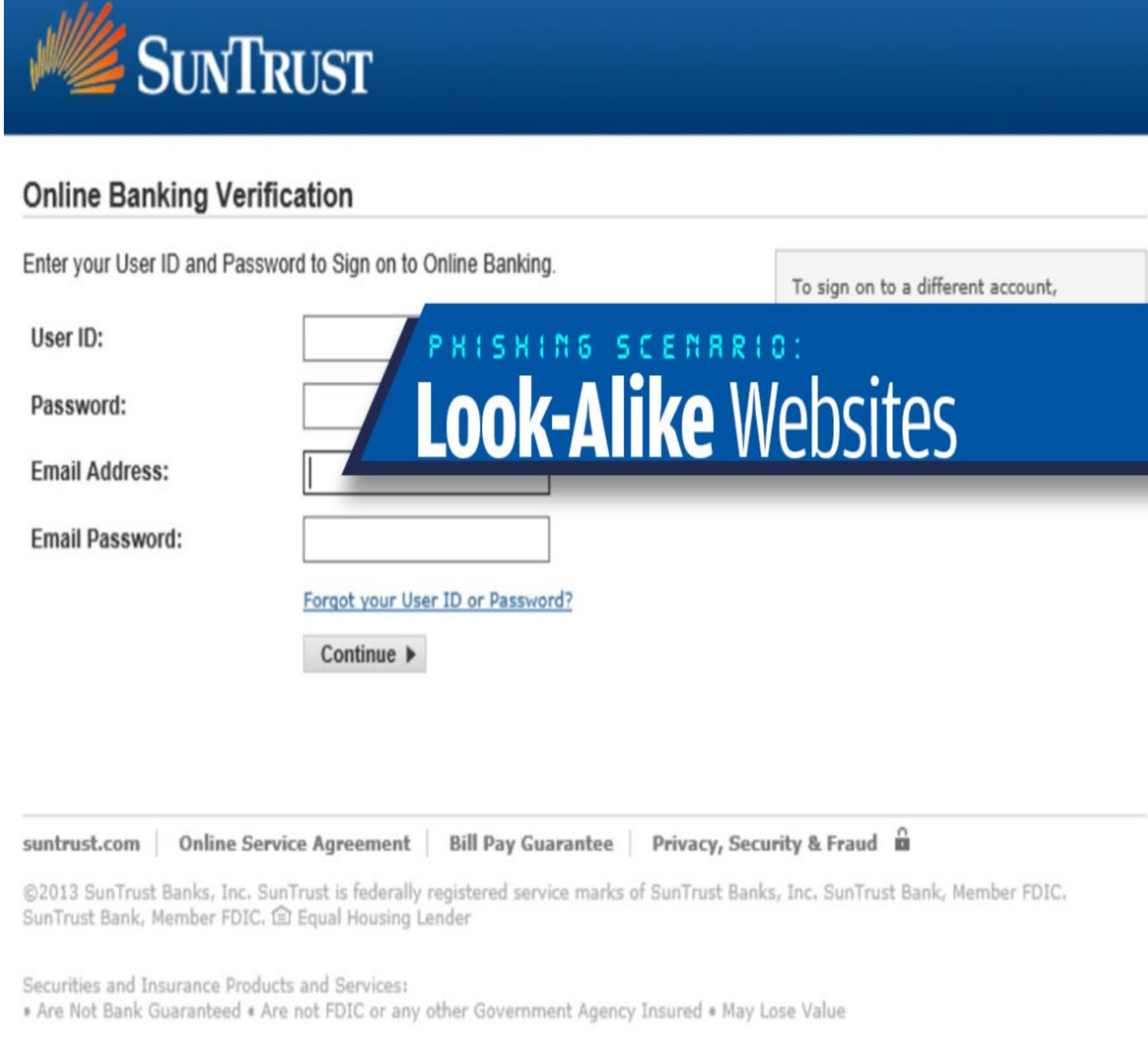
…even people you don’t know.

Phishing

How to Avoid Phishing Scams

Protect your Personal Information:

- To protect yourself from falling victim to a **phishing scam**, it's important to be very careful with your personal information including your usernames and passwords.
- Some *phishing scams* divert you to a fraudulent website designed to look like the website you originally clicked on.
- When you enter your username/password and other information, that information is transmitted to the con artist, who can use it later on.



Online Banking Verification

Enter your User ID and Password to Sign on to Online Banking.

To sign on to a different account,

User ID:

Password:

Email Address:

Email Password:

Forgot your User ID or Password?

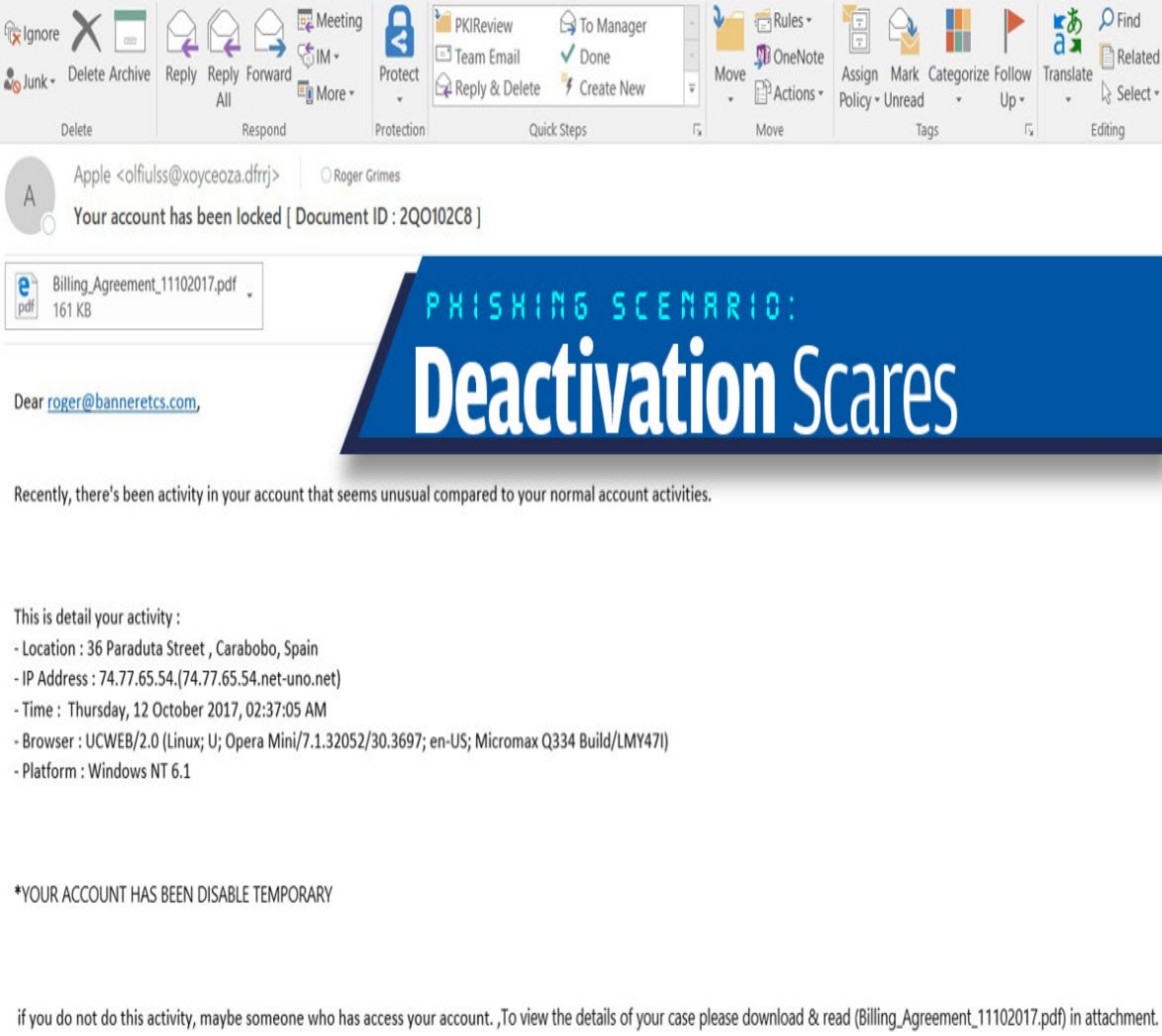
suntrust.com | Online Service Agreement | Bill Pay Guarantee | Privacy, Security & Fraud

©2013 SunTrust Banks, Inc. SunTrust is federally registered service marks of SunTrust Banks, Inc. SunTrust Bank, Member FDIC. SunTrust Bank, Member FDIC. Equal Housing Lender

Securities and Insurance Products and Services:
• Are Not Bank Guaranteed • Are not FDIC or any other Government Agency Insured • May Lose Value

Beware of Suspicious Emails and Do not Click Suspicious Links:

- Be very suspicious of any emails you receive from trusted entities like your bank.
- If the email contains a link, don't click on it.
- Deceptive links that mimic legitimate URL addresses are a common tools con artists use in phishing scams.
- While these addresses may look official, they usually redirect you to a fraudulent site.
- Instead of clicking on the link, type in the web address of the institution into the browser to access the website.



Apple <olfiulss@xoyceoza.dfrj> Roger Grimes

Your account has been locked [Document ID : 2QO102C8]

Billing_Agreement_11102017.pdf
161 KB

Dear roger@banneretcs.com,

Recently, there's been activity in your account that seems unusual compared to your normal account activities.

This is detail your activity :

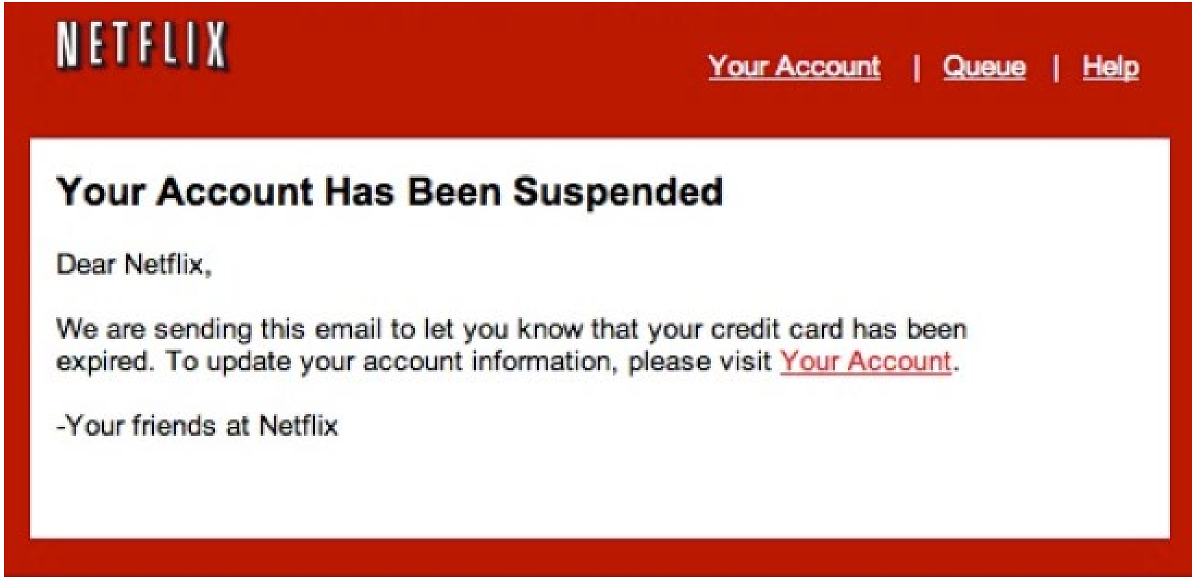
- Location : 36 Paraduta Street , Carabobo, Spain
- IP Address : 74.77.65.54.(74.77.65.54.net-uno.net)
- Time : Thursday, 12 October 2017, 02:37:05 AM
- Browser : UCWEB/2.0 (Linux; U; Opera Mini/7.1.32052/30.3697; en-US; Micromax Q334 Build/LMY47I)
- Platform : Windows NT 6.1

*YOUR ACCOUNT HAS BEEN DISABLE TEMPORARY

if you do not do this activity, maybe someone who has access your account. ,To view the details of your case please download & read (Billing_Agreement_11102017.pdf) in attachment.

Know the Common Phishing Language:

- Look out for common phishing language in emails like "Verify your account."
- Legitimate businesses will not send you an email to ask for your login information or sensitive personal information.
- Also, look out for emails that try to convey a sense of urgency.
- Warnings that your account has been compromised, for example, are a common way to trick victims. Again, contact the company directly to inquire about such emails rather than using any link or other contact information provided in the email.
- Finally, be wary of any email that does not address you directly.
- While some phishing scams will use your name in the email, many are sent out as spam messages to thousands at a time.



Your Account Has Been Suspended

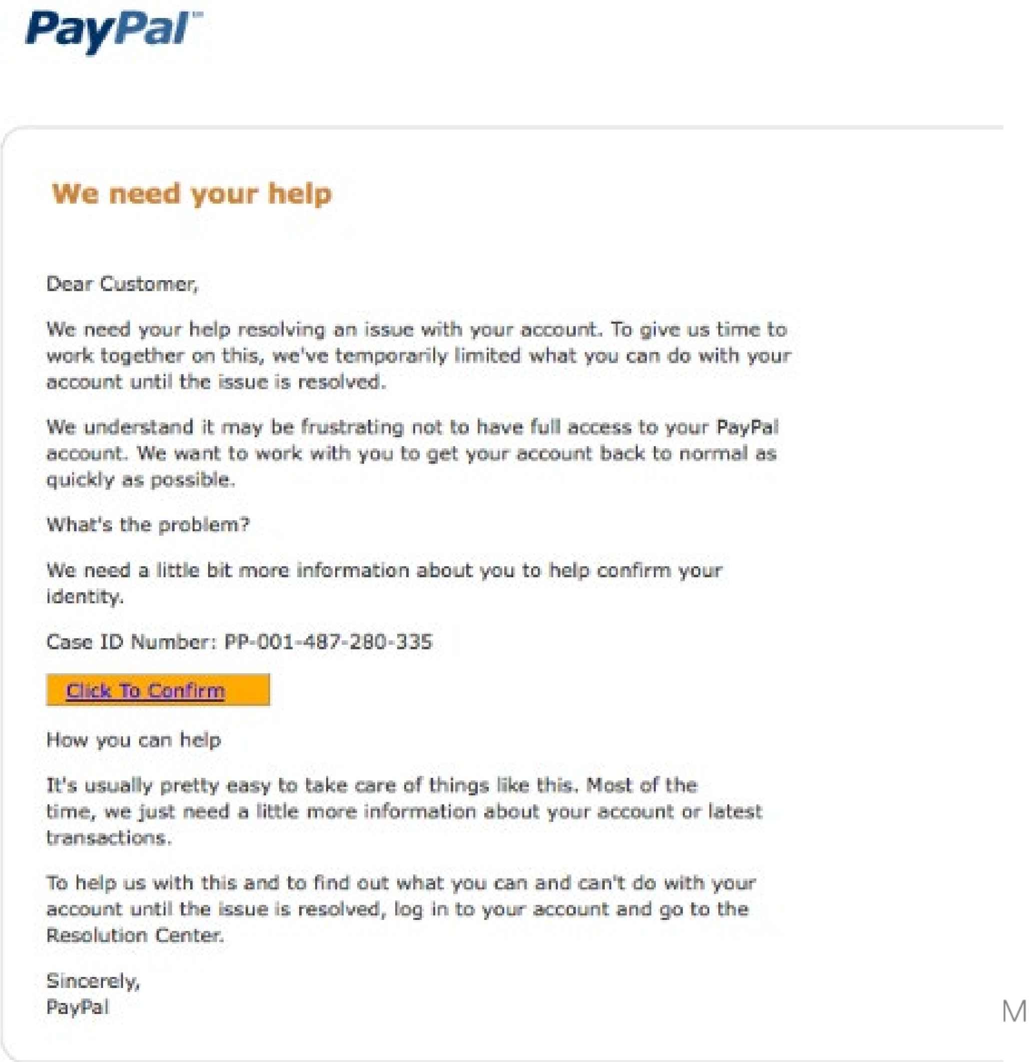
Dear Netflix,

We are sending this email to let you know that your credit card has been expired. To update your account information, please visit Your Account.

-Your friends at Netflix

Count on authenticated websites:

- If you visit a website with a padlock, click on the padlock.
- It should show you the name of the organization that applied for the padlock. If the name does not match the name you know, be very suspicious.



PayPal™

We need your help

Dear Customer,

We need your help resolving an issue with your account. To give us time to work together on this, we've temporarily limited what you can do with your account until the issue is resolved.

We understand it may be frustrating not to have full access to your PayPal account. We want to work with you to get your account back to normal as quickly as possible.

What's the problem?

We need a little bit more information about you to help confirm your identity.

Case ID Number: PP-001-487-280-335

Click To Confirm

How you can help

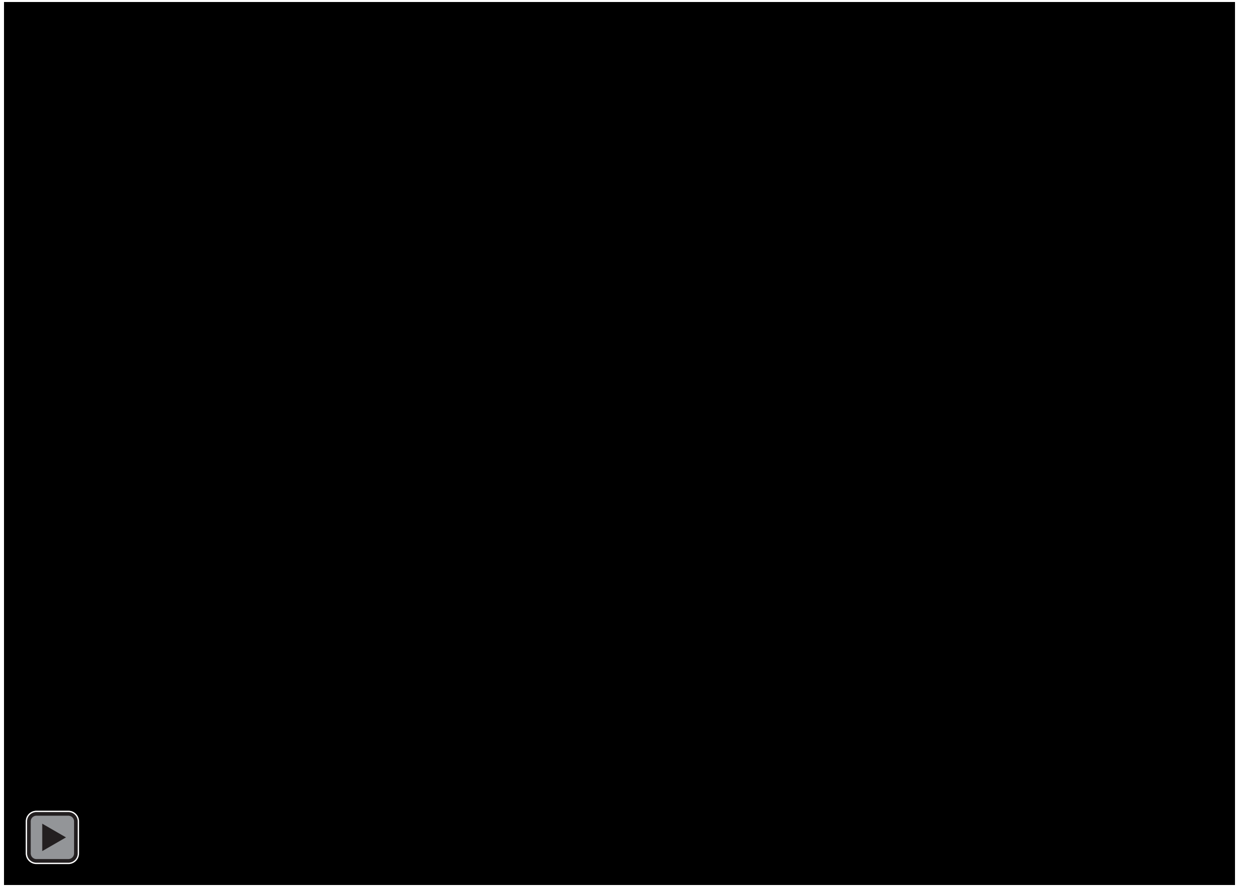
It's usually pretty easy to take care of things like this. Most of the time, we just need a little more information about your account or latest transactions.

To help us with this and to find out what you can and can't do with your account until the issue is resolved, log in to your account and go to the Resolution Center.

Sincerely,
PayPal

VIDEO – Bringing it all together

Cyber Aware



Cyber Aware – Stay Safe Recap

Cyber Safe

Cyber Aware

ALWAYS BE SMART WHEN WEB BROWSING or USING SOCIAL MEDIA APPs

Don't ever disclose personal information. like

Think before you post!

The internet is public.

Cyber Safe

TURN ON YOUR SOCIAL MEDIA PRIVACY SETTINGS

Make your accounts private.

Manually approve any new friends or followers.

Cyber Safe

ONCE YOUR DATA IS OUT THERE ON THE INTERNET ITS NOT UNDER YOUR CONTROL.

Any photo that's uploaded is the property of that website.

Uploading a bad picture and deleting it a few minutes or seconds later doesn't change this.

The Internet is a fantastic invention, enjoy it but stay Cyber Aware

Cyber Aware