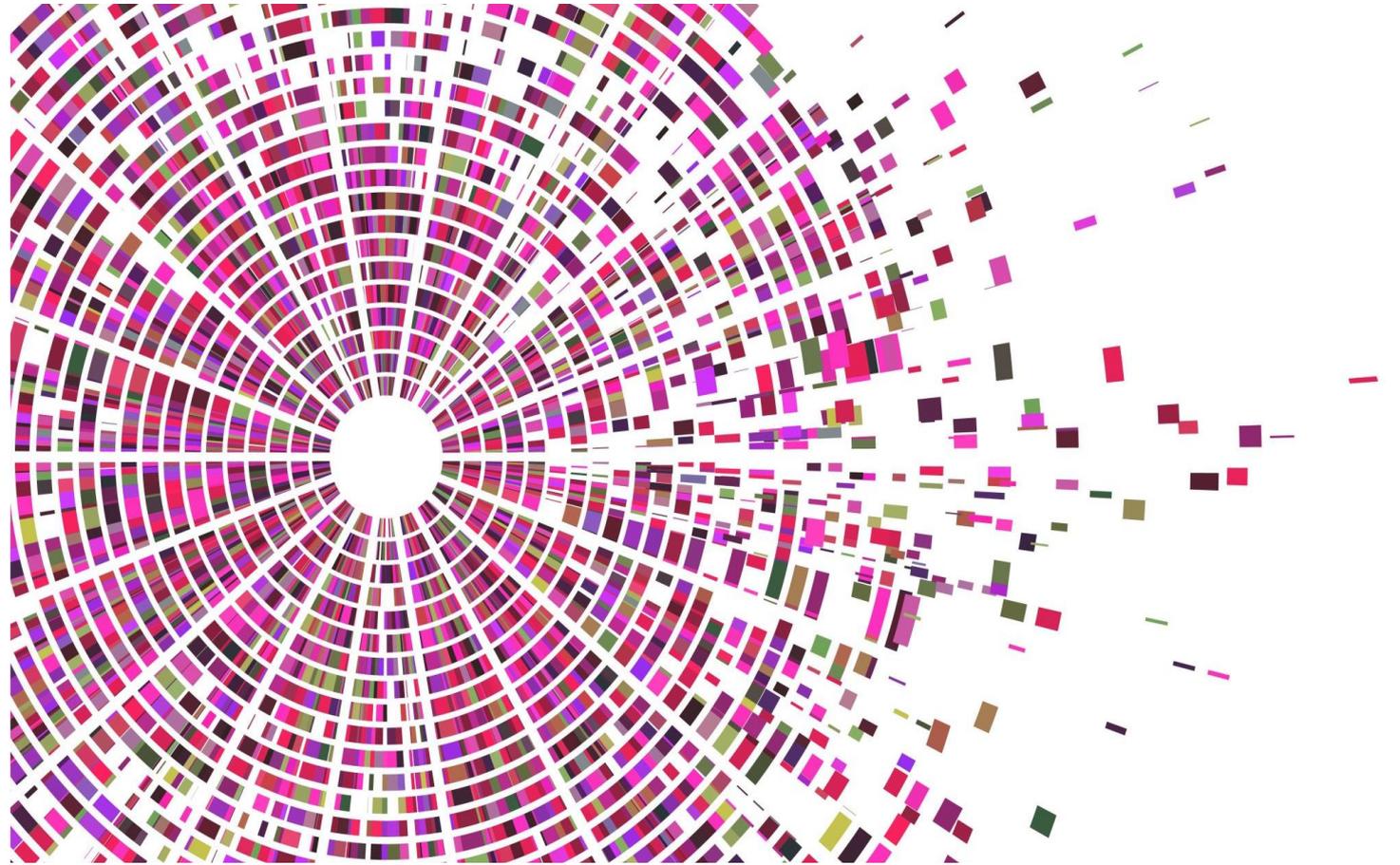


Internet Safety

PROTECTING YOURSELF IN THE
DIGITAL WORLD



The background of the slide features a stylized illustration of a diverse group of people. The figures are rendered in various colors (blue, green, yellow, pink, purple) and are shown from the chest up, with their hands raised in the air. This visual metaphor represents an active and engaged classroom environment. The overall color palette is vibrant and modern, set against a dark blue background.

Classroom Agreements

Our class works the best when we...

- Raise hand before speaking
- Avoid interrupting others
- Don't eat in class
- Turn off cellphones and put them away

Course Overview

In this class we will cover the following topics:

Introduction and Social Networking overview

Facebook-Online friendship boundaries (What is appropriate? What is inappropriate?)

Safe Practices- Scams, Predators

Safe Practices-Viruses

Course Overview

In this class we will cover the following topics:

Shopping online

The Internet as a tool- Recreation, News, Education and Employment

Internet as a tool: Fact finding, reliable resources and plagiarism (stealing other people's words and using them as your own)

Review

The internet can be accessed in different ways.



How many can you name?

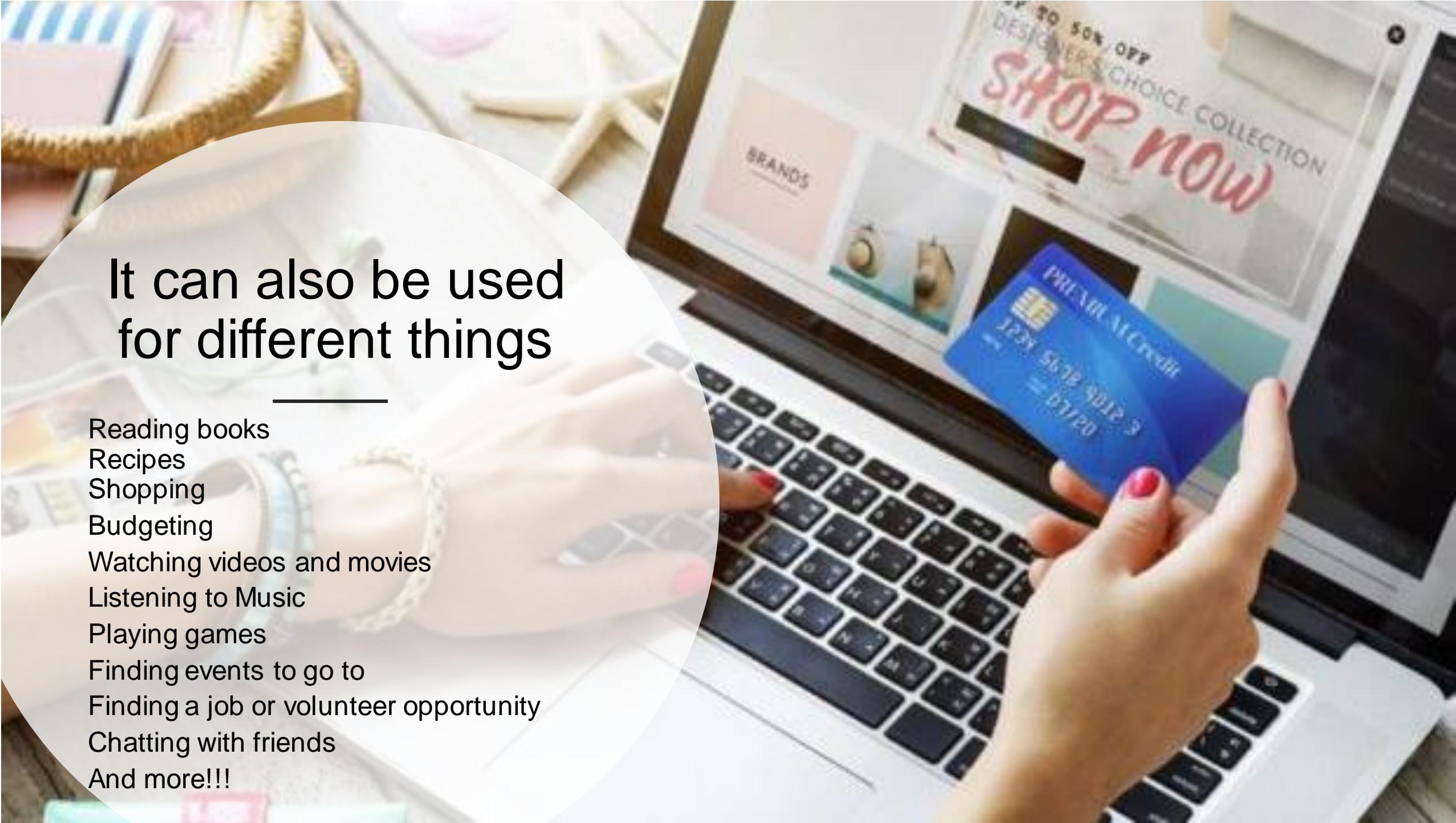
Computer

Laptop

Smart Phone

Kindle

Tablet



It can also be used for different things

- Reading books
- Recipes
- Shopping
- Budgeting
- Watching videos and movies
- Listening to Music
- Playing games
- Finding events to go to
- Finding a job or volunteer opportunity
- Chatting with friends
- And more!!!



Today we will
begin to take a
look at Social
Networking

What is Social Networking?

Social networking is when you use an application on a smart phone, computer or other device to interact with people and or businesses.





Social networking is a way
to reach out to other people

You can use it to keep in touch with friends around the world.

You can talk to other people who share your interests.

You can share ideas and advocate for things you care about.

You can play games with other people

and more...

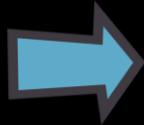
However:

KNOW THE FACTS TO KEEP YOUR KIDS SAFE



Adults and children need to be aware it's not always safe.

75% of youth who received an online sexual solicitation did not tell a parent

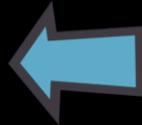


There is estimated to be over **5,000,000** predators that surf the internet

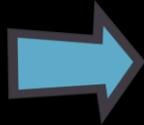
64 percent of the teens surveyed admitted they did things online that they would not want their parents to know about

14%

have actually met face to face with a person they have met on the Internet



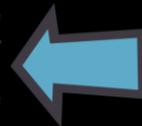
75% of kids are willing to share personal info online about themselves and their family in exchange for goods and services



Nearly **75%** of victims who met offenders face-to-face did so more than once

77%

of the targets of online predators were 14 or older



22%

were between the ages of 10 and 13

9 out of 10

parents will NEVER KNOW that any INAPPROPRIATE CONTACT has occurred



MySpace **DELETES** an average of **45,000 accounts** per year of **registered sex offenders**

Not everyone online is a nice person.

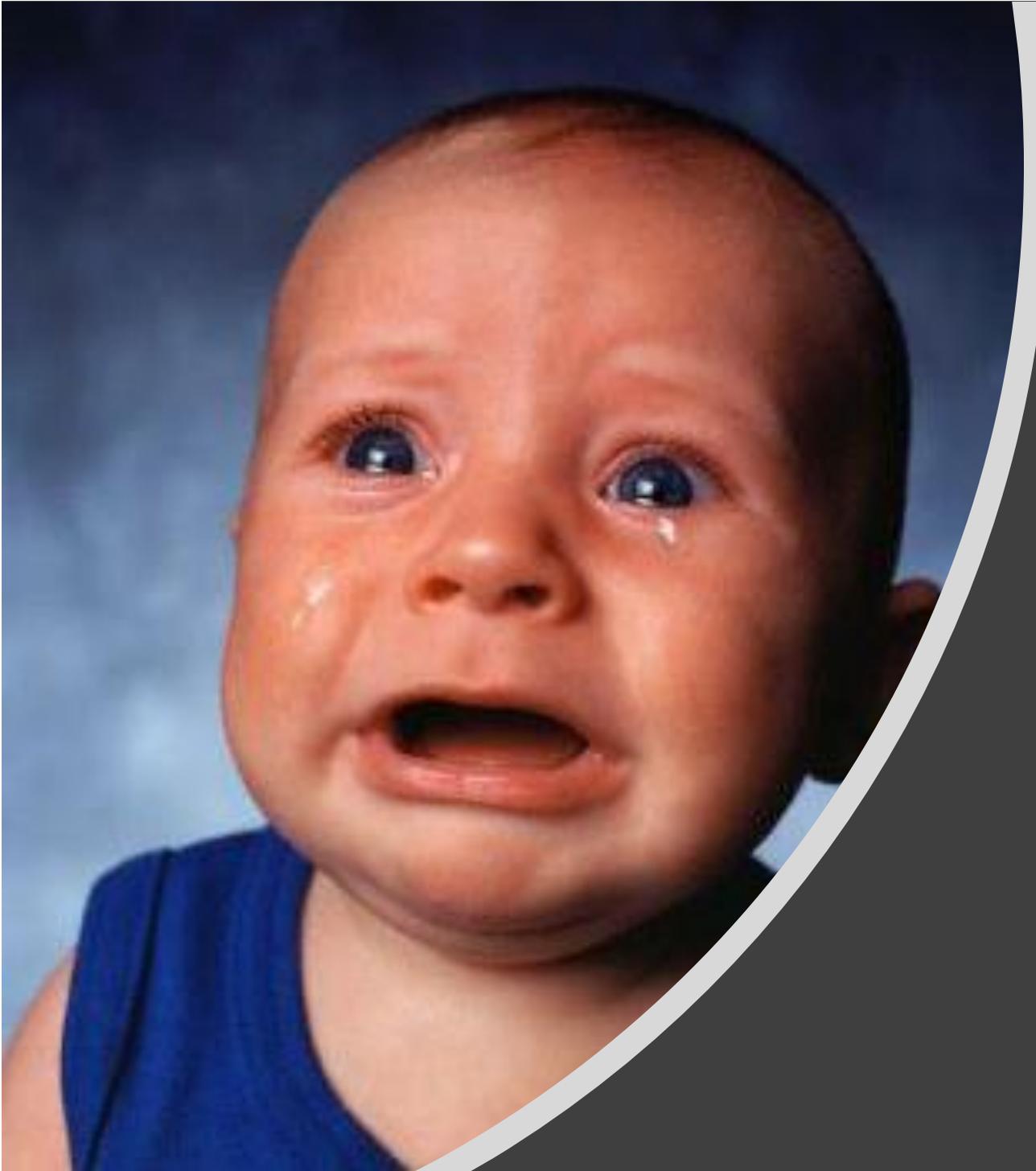
There are people who are up to no good and want to take your money, your stuff or you.

How can you keep yourself safe?

References:
The Pew Charitable Trusts <http://www.pewtrusts.org/>
PC's n Dreams <http://www.pcndreams.com>
Online Safety Tips <http://www.onlinesafetytips.com>
Edine Articles <http://EdineArticles.com/4615801>
Designer: Brigit Gilbert

This Photo by Unknown author is licensed under [CC BY-NC-ND](https://creativecommons.org/licenses/by-nc-nd/4.0/).

TO LEARN MORE ABOUT CHILD PREDATORS
AND HOW TO PROTECT YOUR CHILD VISIT:



And it's easy to
fall into
disagreements
with friends

Even when you don't
mean to.

So, how do
we use Social
Media
responsibly?

And safely.

Before you speak:

T H I N K

T = Is it True?

H = Is it Helpful?

I = Is it Inspiring?

N = Is it Necessary?

K = Is it Kind?

How can YOU best keep yourself, your information and your identity safer?



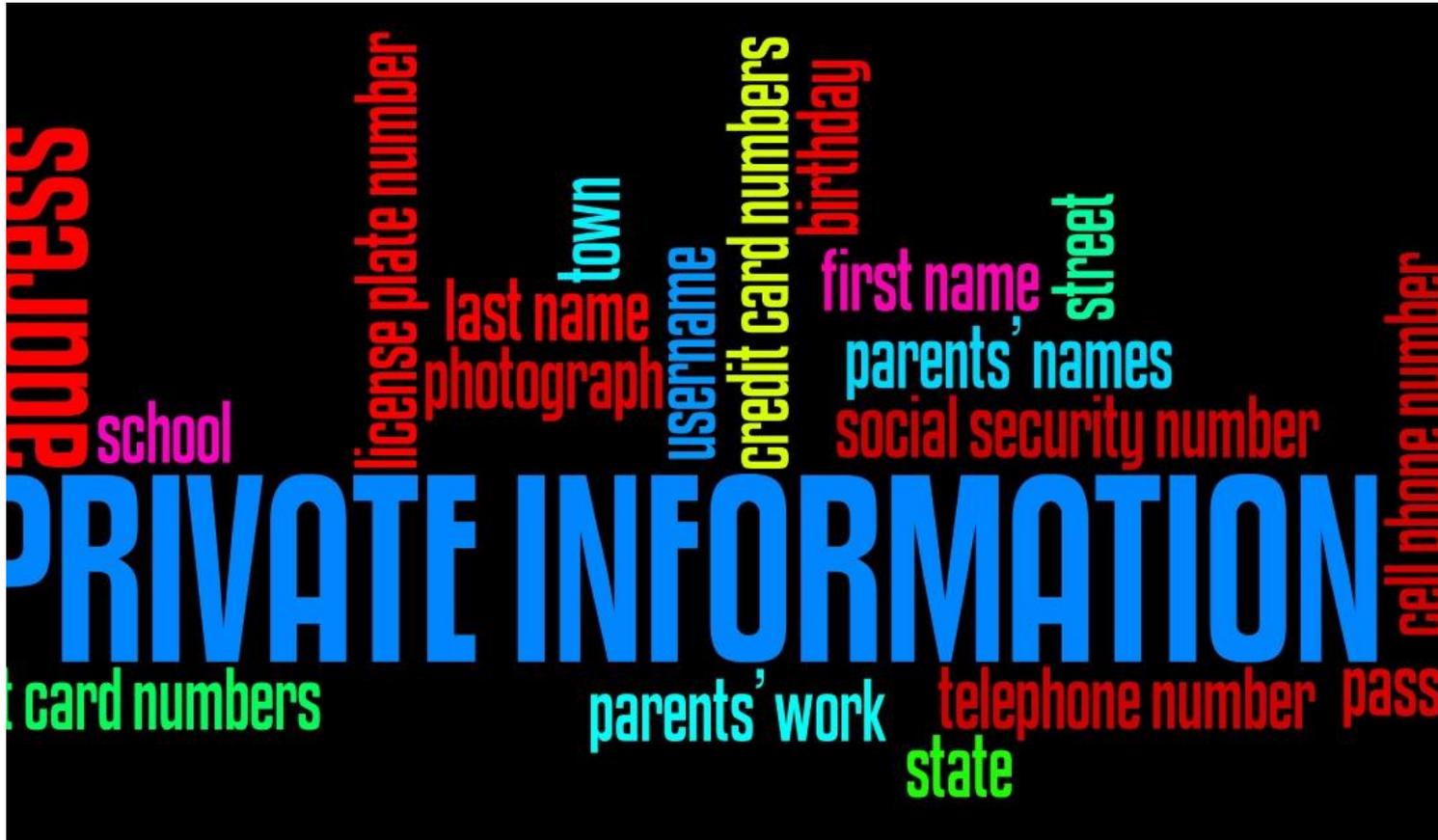
Identity
Theft
precautions

Visit

ftc.gov/idtheft

To Learn More About Protecting Your Identity





Facebook

Whenever you sign up for an account on any social media site, you are agreeing to allow them to use your personal information. This includes what you are looking at, and anything you post, including your photographs.

There is no way to set up an account without clicking on an agreement which allows them to do this. It is the price we pay for a free account.

Next are some ways you can protect your account from sources outside of the social media site itself.

Can the Spam

Spam is not just a canned meat product. ~~It also means sending out the message to lots of people (usually strangers) generally trying to sell you something. Usually this is in an Email or Private message.~~ *Spam* is generally email advertising for some product sent to a long mailing list or newsgroup.

Its best to delete these messages and not open them. Some may contain computer programs called Malware or Viruses. (Mal in Latin means bad- basically it's a program that goes into your computer to cause problems)

DO NOT SEND IT TO ALL YOUR FRIENDS even if it tells you to- Its annoying. And do you want to send your friends something that can potentially harm their computer?





Don't share personal
information

- Some information like your credit card, Birthday, Mothers Maiden name, Social security number, bank account and State ID number could allow someone to pretend to be you and use this information to have access to your money, open other accounts in your name.



Lets explore a website to see how we can keep our accounts safer.

<https://usa.kaspersky.com/resource-center/threats/facebook-identity-theft-prevention>



Don't share your
password

Your password allows you to access your account. If you share it with anyone they can log in and pretend to be you.

If you need a note to remember it by, keep it somewhere safe.



Do not access or post in someone else's account profile- Always log out so no one can use yours!

A **Facebook profile** is an individual's personal **account**, where he or she can post updates, upload photos, share videos, maintain a friends list and provide personal information.

Would you want someone else to pretend to be you and speak for you?

Its like stealing someone else's identity.

Privacy settings

The screenshot shows the Facebook 'Privacy Settings and Tools' page. On the left sidebar, the 'Privacy' menu item is highlighted with a red arrow. The main content area is titled 'Privacy Settings and Tools' and contains several sections:

- Who can see my stuff?** (with a red arrow pointing to the section title)
- Who can see your future posts?** (with a red arrow pointing to the 'Friends' dropdown menu in the post creation area). The dropdown menu is open, showing options: Public, Friends (checked), Only Me, Custom, Close Friends, Triberr, and See all lists...
- Who can look me up?**

Other visible elements include a 'Post' button, 'Use Activity Log' link, and 'Limit Past Posts' link.

Be sure to set your privacy settings on your facebook account to be in charge of who gets to see your information.

Firewall

A firewall is a program that runs on your device that blocks most malware and protects it from computer viruses which can do damage to your device, collect data including passwords and bank or personal information. Think of them as a vaccine for your device.

As mentioned before, Malware is a program meant to steal information or harm your computer. A computer virus is a type of malware.

These need to be regularly updated as new versions come out to protect your device from new threats.



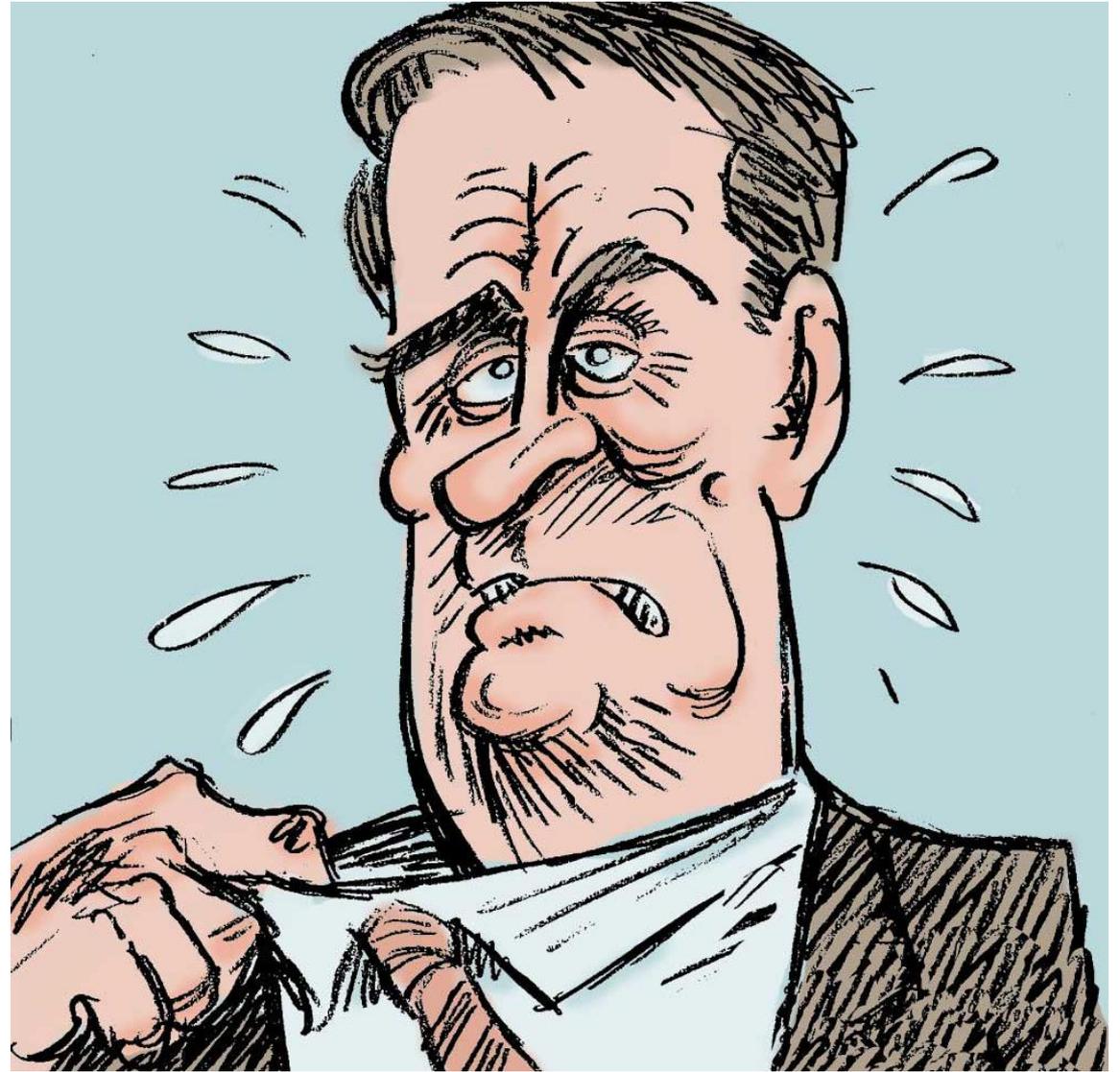
Nothing you post is private

Don't post anything you would not want your parents, a child, or your boss to see.

People have lost jobs friends and opportunities from posting things they regret.

If you would not say it to someone directly, it's not a good idea to post it.

Once it is posted, even if you delete it, someone could have saved a screenshot





Lets watch a short video about internet safety. It's geared for teens- but most of it applies to all of us!



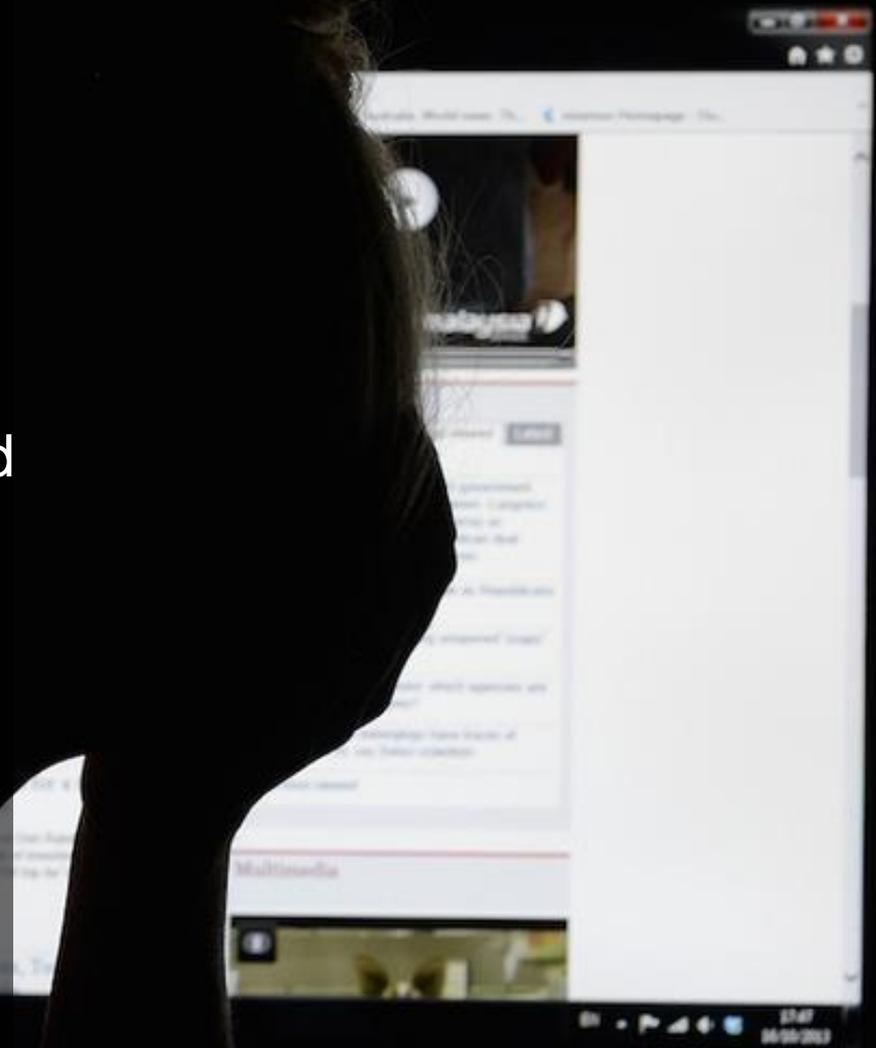
Cyber bullying

Do not bully, harass or intimidate other people online. This is called Cyber bullying.

Do not post pictures which contain nudity, violence or sex.

These things will get your account shut down and you will not be able to use facebook. In some cases, it is also breaking the law, and you could go to jail.

It's just not right to do!



"Cyber bullying can make you feel totally overwhelmed which can result in many feeling embarrassed that they are going through such a ~~devastating time, and not~~ knowing what support is available to them."

Its important to tell someone in your circle of support if you are being bullied.

Source:
<https://www.bullying.co.uk/cyberbullying/effects-of-cyberbullying/>



How you can support someone being cyberbullied



- Tell them that no one deserves to be treated in this way and that they have done nothing wrong
- Ensure that they know that there is help available to them
- Encourage them to talk to someone that they trust so they feel they have somewhere safe to go to
- Encourage them to talk to their parents/carers and if this isn't possible to write a letter or speak to another family member
- Take screen shots of the cyber bullying so that they have proof this is happening



Continued Cyberbully support
(from <https://www.bullying.co.uk/cyberbullying/effects-of-cyberbullying/>)

- Report all abuse to the relevant [social media networks](#) by clicking on the “report abuse” button
- Keep a diary so they have somewhere safe and private to write down their innermost thoughts and feelings which will help to avoid feelings bottling up
- Give praise for being so brave and talking things through which will hopefully empower them to take responsibility and get help

DRAMA





Post as if someone was posting about YOU

- Would you want someone sharing your story without your permission?
- Do you want people talking about the mistakes you made publicly using your name?

remember THINK from before? Its a good rule to review before you hit POST.

Remember: Before you press POST

Before you speak:

T H I N K

T = Is it True?

H = Is it Helpful?

I = Is it Inspiring?

N = Is it Necessary?

K = Is it Kind?

Do not make up stories about yourself that are not true for your profile

Putting false information on your profile is against Facebook rules. Your account can be shut down for it.

Your account can be shut down if you put false information (also called Misrepresenting yourself) on your profile.

Remember this saying: "Lies have fast little legs, and have very sharp teeth. They will catch you and bite you in the rear."
Yes, Actions have consequences. Adding a lie on top of a mistake never makes the consequences easy.



Hate Speech can get you banned!



This Photo by Unknown author is licensed under [CC BY-NC](#).

The following groups are protected from people making threats about them based only on the fact they are part of one of these groups.

Protected classes

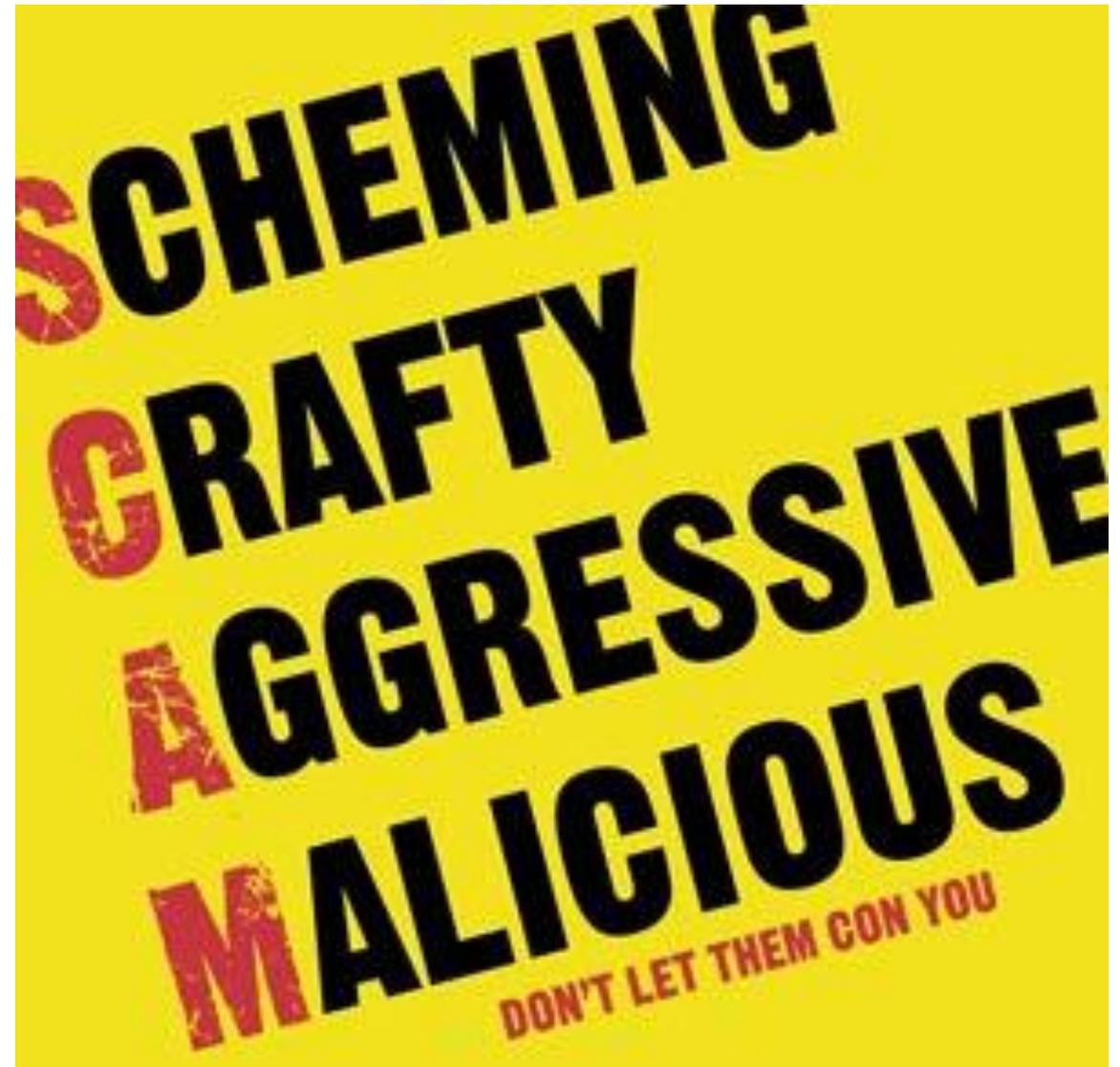
- [Race](#) – [Civil Rights Act of 1964](#)
- [Religion](#) – [Civil Rights Act of 1964](#)
- [National origin](#) – [Civil Rights Act of 1964](#)
- [Age](#) (40 and over) – [Age Discrimination in Employment Act of 1967](#)
- [Sex](#) – [Equal Pay Act of 1963](#) and [Civil Rights Act of 1964](#)
 - The [Equal Employment Opportunity Commission](#) interprets 'sex' to include discrimination based on [sexual orientation](#) and [gender identity](#)^[2]
- [Pregnancy](#) – [Pregnancy Discrimination Act](#)
- [Familial status](#) – [Civil Rights Act of 1968](#) Title VIII: Prohibits discrimination for having children, with an exception for senior housing. Also prohibits making a preference for those with children.
- [Disability](#) status – [Rehabilitation Act of 1973](#) and [Americans with Disabilities Act of 1990](#)
- [Veteran](#) status – [Vietnam Era Veterans' Readjustment Assistance Act of 1974](#) and [Uniformed Services Employment and Reemployment Rights Act](#)
- [Genetic information](#) – [Genetic Information Nondiscrimination Act](#)

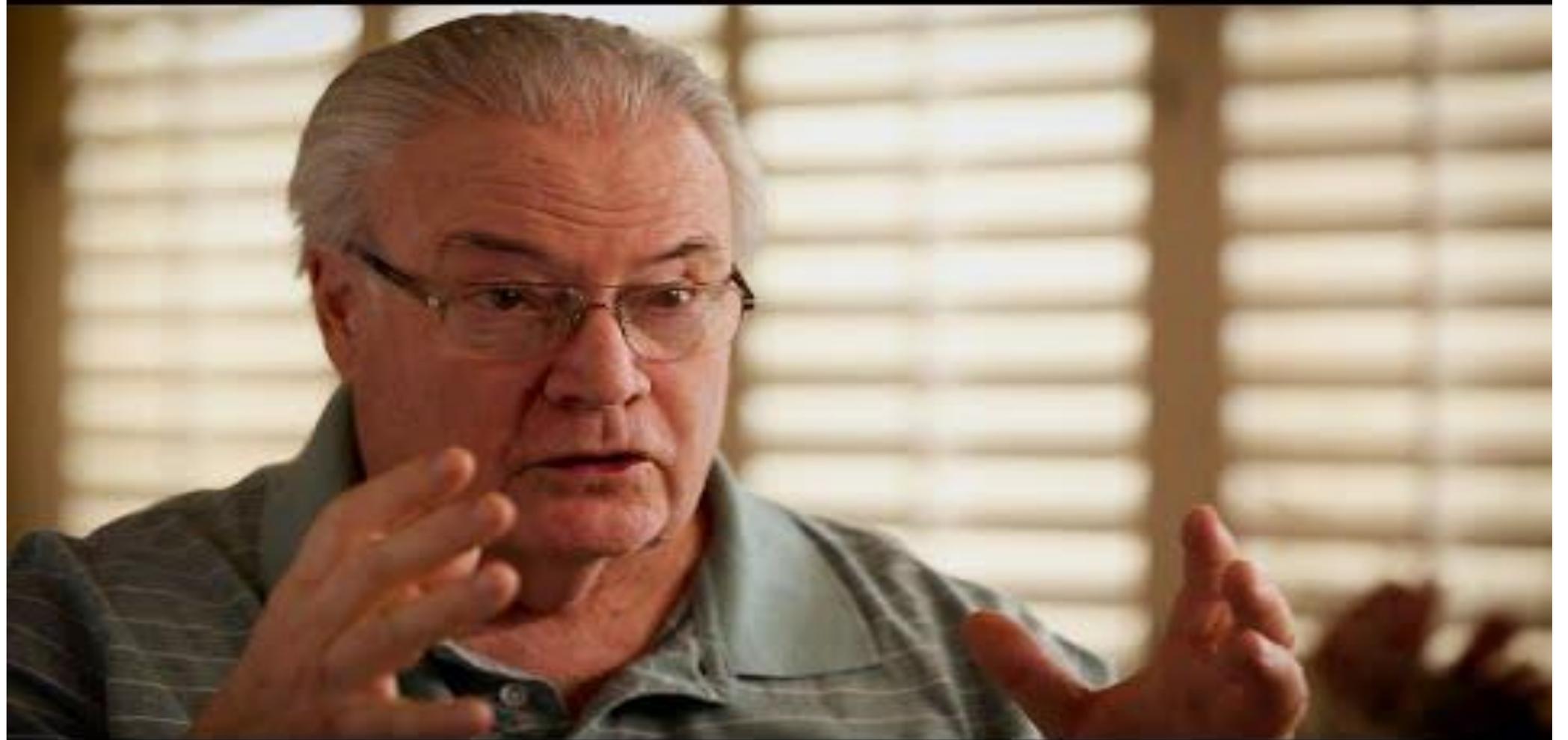


Scammers

A scammer is a person trying to gain something of value from you. Like Bank information, Money , your information so they can open a line of credit in your name, even you.

There are many different types of scammers on the internet.







Let's check out
another website.
Ten most
common scams
worldwide

<https://nt.gov.au/law/crime/scams/ten-most-common-types-of-scams>

Wait! GO back. Let's follow the link that says "How to protect yourself"

<https://nt.gov.au/law/crime/scams/protect-yourself-from-scams>

Hello!

As part of our security measures, we regularly screen activity in the Facebook system. We recently contacted you after noticing an issue on your account.

Spelling

Our system detected unusual Copyrights activity linked to your Facebook account , please follow the link bellow to fill the Copyright Law form:

http://www.facebook.com/application_form

Links in email

Note: If you dont fill the application your account will be permanently blocked.

Threats

Regards,

Facebook Copyrights Department.

Popular company

What safety tips do you follow?

stay safe online

Remember the 5 SMART rules when using the Internet and mobile phones.

S

SAFE: Keep safe by being careful not to give out personal information – such as your full name, email address, phone number, home address, photos or school name – to people you are chatting with online.

m

MEET: Meeting someone you have only been in touch with online can be dangerous. Only do so with your parents' or carers' permission and even then only when they can be present.

a

ACCEPTING: Accepting emails, IM messages, or opening files, pictures or texts from people you don't know or trust can lead to problems – they may contain viruses or nasty messages!

r

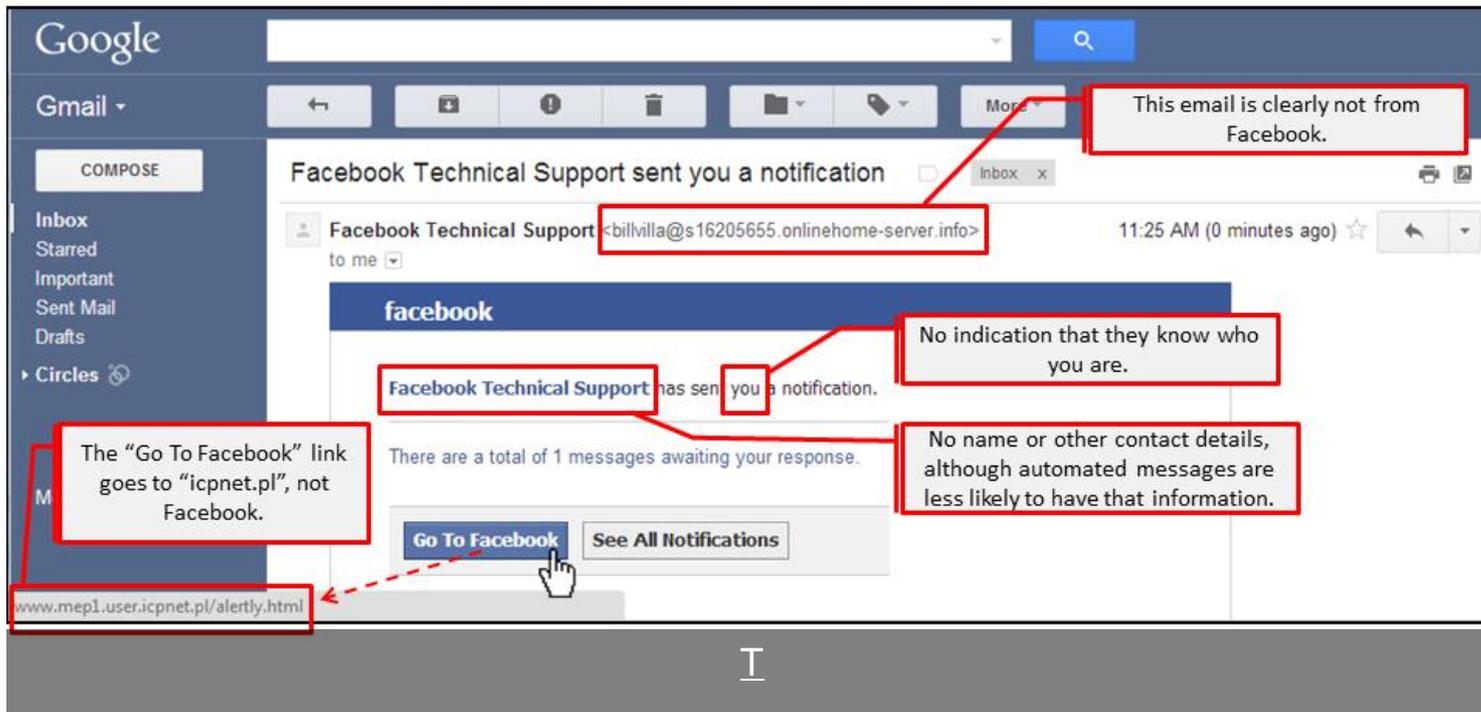
RELIABLE: Information you find on the internet may not be true, or someone online may be lying about who they are. Make sure you check information before you believe it.

t

TELL: Tell your parent, carer or a trusted adult if someone or something makes you feel uncomfortable or worried, or if you or someone you know is being bullied online.

Find out more at [Childnet's website](#) ...

This Photo by Unknown author is licensed under [CC BY-SA-NC](#).



Phishing

- There are several ways your information can be stolen. Phishing is when someone comes up with a scheme to get your private information such as bank or credit card number to use them to buy things or open accounts in your name.

Some emails from companies look real- but are fake.

Subject: Intuit Payroll Confirmation inquiry.
Date: Thursday, September 27, 2012 8:17:14 AM Pacific Daylight Time
From: Intuit PaymentNetwork <lotusq260@realliving.com>
To: [REDACTED]@ucdavis.edu
Priority: High

"From" address doesn't match purported sender.



Direct Deposit Service System information

Status update

Respectively [REDACTED]@ucdavis.edu
We received your payroll on September 27, 2012 at 1:14 AM EST.

Fake bank account number, listed

- Funds will be withdrawn from the bank account number: 8 - 9513 on September 28, 2012.
- Amount to be withdrawn: \$1,555.26
- Paychecks will be transferred to your employees' accounts on: September 28, 2012
- Please review details of your payroll [here](#).

Use of threats

Funds are typically processed before normal business hours and are not accessible by 12 AM EST on the date funds are available. <http://kohimeka.hspps.net/wp-content/plugins/zloroomonoo/iqbprpc.html>

Intuit must serve your payroll by 5 p.m. EST, two banking days before your paycheck date or your employees will not be paid regarding your schedule. QuickBooks does not proceed payrolls on weekends & federal banking holidays. A list of federal banking free days can be downloaded at the [Federal Reserve non-working days schedule](#).

Thank you for your business.

"Hovering" cursor over link shows unexpected destination

Sincerely,
Intuit Payroll Support

IMPORTANT NOTICE: This notification is being sent to inform you of a transactions mentioned in your account. Please mind that if you agreed with terms of receiving marketing materials from Intuit Services you may continue to receive informational letters similar to this message that aim your service or software.

phishing page uses http, and gmail uses https.

be smart and tackle this :)

on gmail.com this always changes , but not on this phishing page

©2009 Google - [Gmail for Organizations](#) - [Gmail Blog](#) - [Terms](#) - [Help](#)



Do not allow a 3rd party to remote into your computer to fix it- this is how they can see everything you do online!



This Photo by Unknown author is licensed under [CC BY-NC-ND](#).

So now we know

1. Don't tell strangers who call you any information about your personal address, birthday, credit card or bank card
2. Don't let them log into your computer remotely. Microsoft and the IRS will not call your phone!! You will not go to jail for hanging up.
3. Program the people you know into your phone contacts. If a number you do not know shows up, do not answer it.
4. Be wary of fake emails. No long lost relative you've never heard of needs your bank info to send you money.
5. If you are buying something online, make sure it is a secure site. (That the web address begins with https://)



Whew! After all that you might be a wondering "Is it worth it"

The internet can be used in a lot of great ways too.

What are your favorites?

Take the next 3 minutes to write down what you use the internet for? Can you think of at least 3?

Lets take a few minutes and share them.

Though the internet has its dangers, it also has its rewards.

Post selfies

Listen to Music

Share ideas

Advocate for causes you believe in

Play games

Share resource information

Learn about local events

Create your own event

Share recipes

Share a poem

Show off your art

Express your thoughts

Shop

Make friends

Keep in touch with distant friends and relatives



What things
do you use
the internet
for?

Connecting with People!