ONLINE SAFETY

Nekoosa Help Desk Lesson #5
Online Safety

Today we will be covering...

- Surfing the Web Safely
- Password Management
- Identifying False Info
- Social Media Safety

Today's Lesson

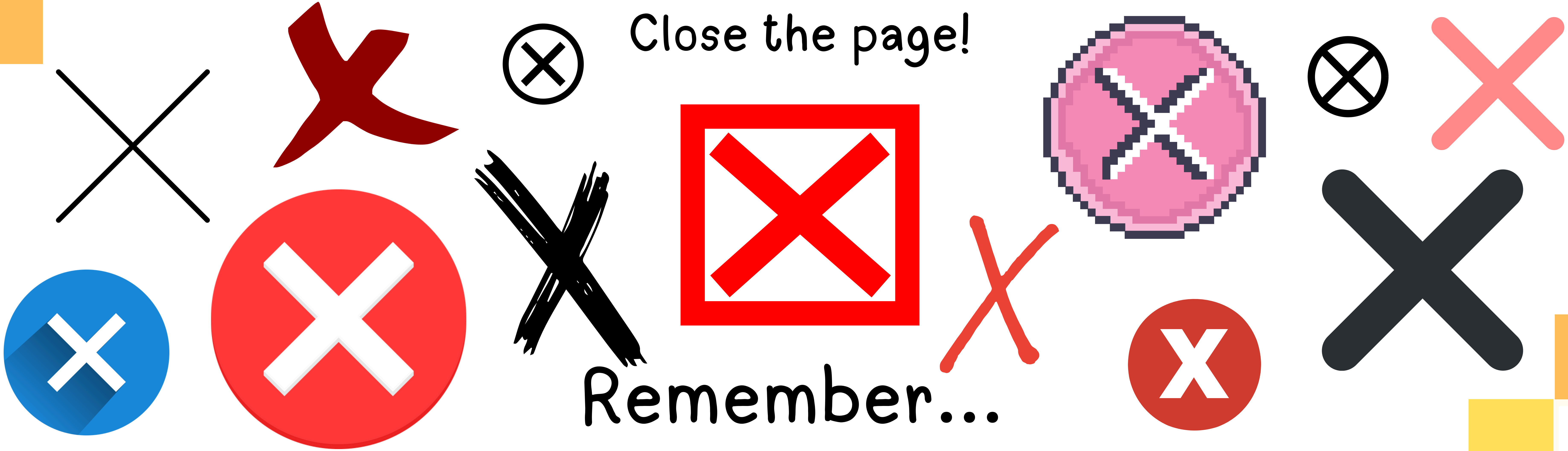
If you take away nothing else from this presentation...

DO NOT CLICK ON ADS & POP UPS

Your Best Friend is the X Button

They can look different, but they all do the same thing:

Close the page!



Remember...

When in doubt, close it out!

Surfing Safely

Using a Secure Browser

To start looking things up on the internet, you will need a browser. There are many options, but it is best practice to use a reputable one.

Web Browsers

These are the most popular browsers. All of these are reliable and update their safety software regularly.

Google Chrome

https://en.wikipedia.org/wiki/Google_Chrome

Microsoft Edge

https://commons.wikimedia.org/wiki/File:Microsoft_Edge_logo_%282019%29.svg

Mozilla Firefox

https://en.wikipedia.org/wiki/Firefox

Safari

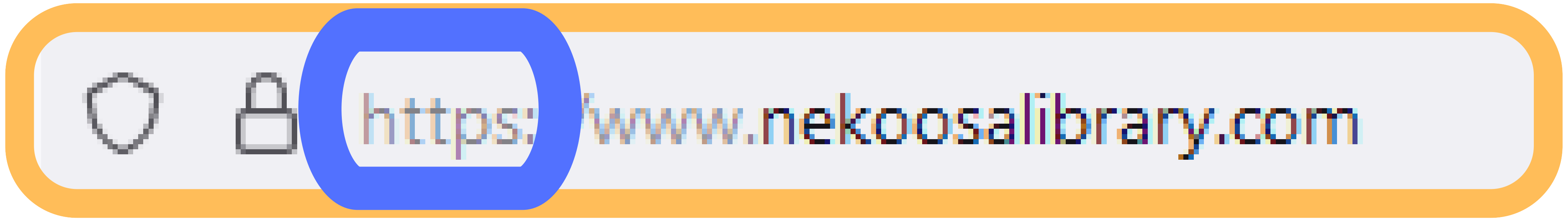
https://logos.fandom.com/wiki/Safari_(iOS)#2017%E2%80%93present

What Sites to Trust

There are TONS of websites on the internet. Some are more fishy than others. Here are a few tips and tricks to help you find the good ones.

Secure Sites

Not all websites are built the same! Some websites use a security measure called "encryption" to make it more difficult for hackers to identify the data that gets sent to and from their website. A secure website will always start with an https. Unsecured websites use http... so stick to websites with the s!



https://www.nekoosalibrary.com

Ads Everywhere!

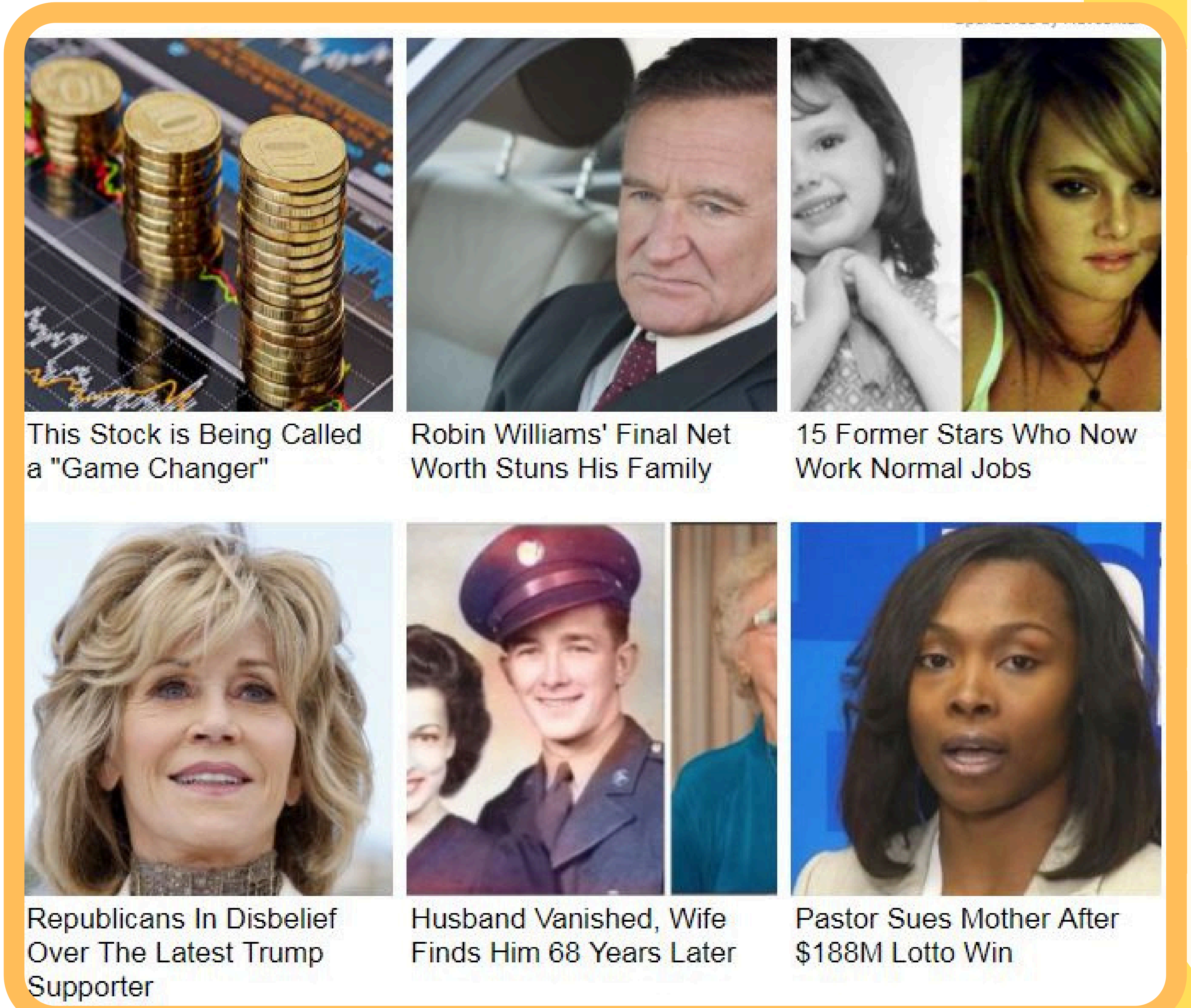
Some sites have lots obnoxious ads. Ads exist simply to get you to click on them. They can be eye catching news articles, cool new products, software download buttons, etc. While a lot of ads are harmless and just exist to make money, many are scams, and some can even download viruses to your computer. It's best not to click on ads.

Personal Information

As a general rule of thumb, never enter any personal or identifying information online. Some ads will lead you to sites that ask for emails, phone numbers, addresses, and even social security numbers. Do not enter any of this information into a website you don’t trust, and close the site if it seems suspicious.

Clickbait

Clickbait is a type of ad made specifically to catch your attention and make you click it. These are often news articles headlines on Facebook. These ads can often show false information on fake news sites. Don't click on these.



This Stock is Being Called a "Game Changer"

Robin Williams' Final Net Worth Stuns His Family

15 Former Stars Who Now Work Normal Jobs

Republicans In Disbelief Over The Latest Trump Supporter

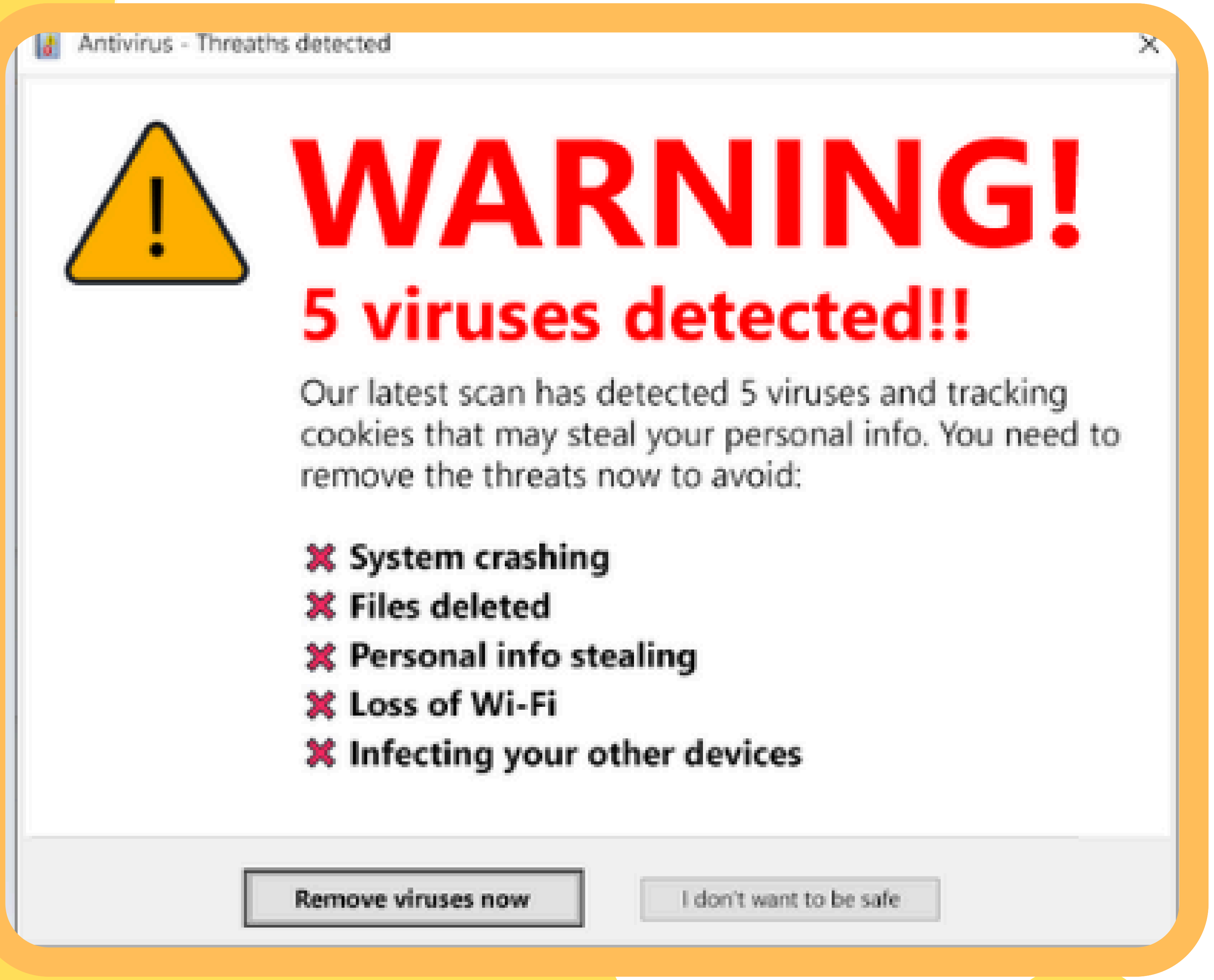
Husband Vanished, Wife Finds Him 68 Years Later

Pastor Sues Mother After $188M Lotto Win

https://www.politifact.com/article/2017/oct/04/more-outrageous-better-how-clickbait-ads-make-mone/

Scary Pop Ups

Some ads are pop ups designed to scare you. These are FAKE and should be closed.



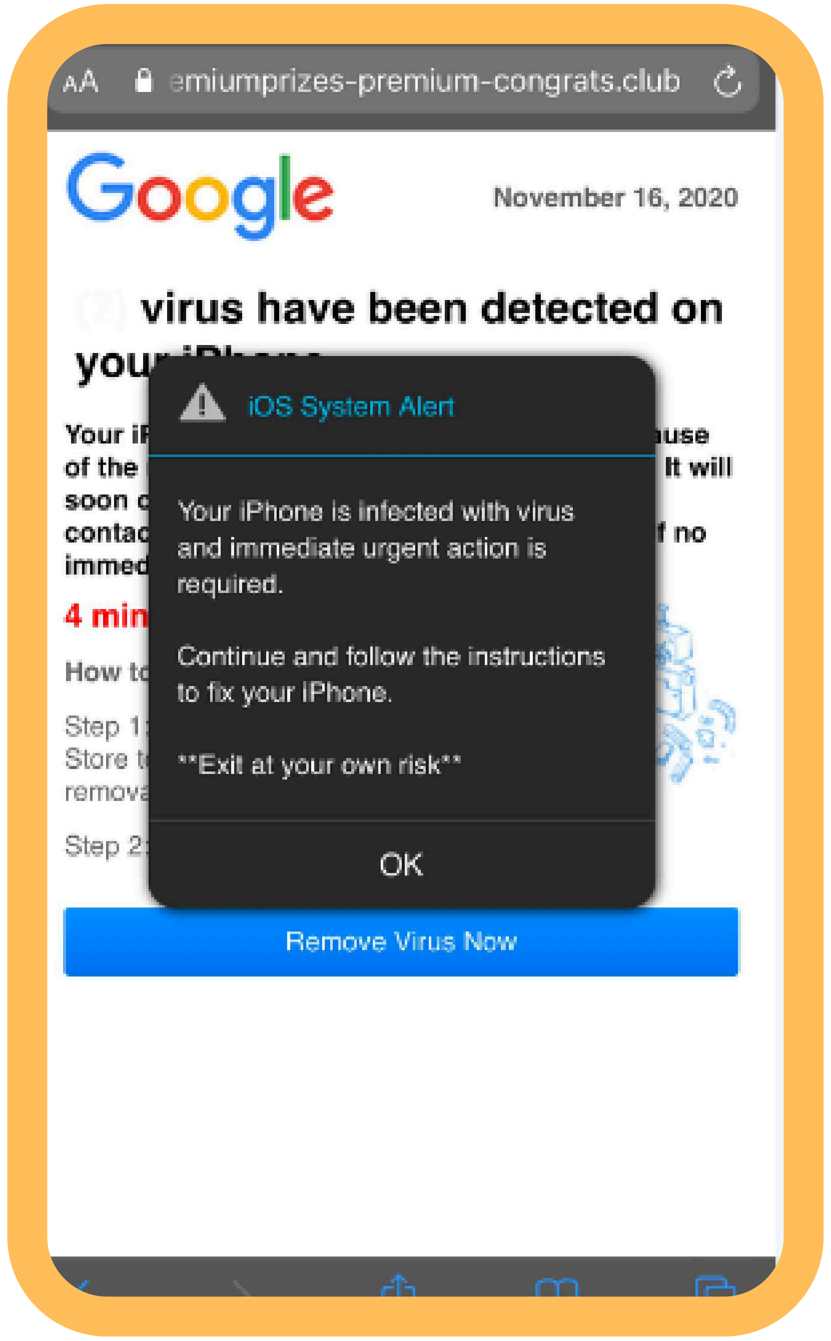
Antivirus - Threaths detected

WARNING!

5 viruses detected!!

Our latest scan has detected 5 viruses and tracking cookies that may steal your personal info. You need to remove the threats now to avoid:

- ✖ System crashing
- ✖ Files deleted
- ✖ Personal info stealing
- ✖ Loss of Wi-Fi
- ✖ Infecting your other devices



emiumprizes-premium-congrats.club

Google November 16, 2020

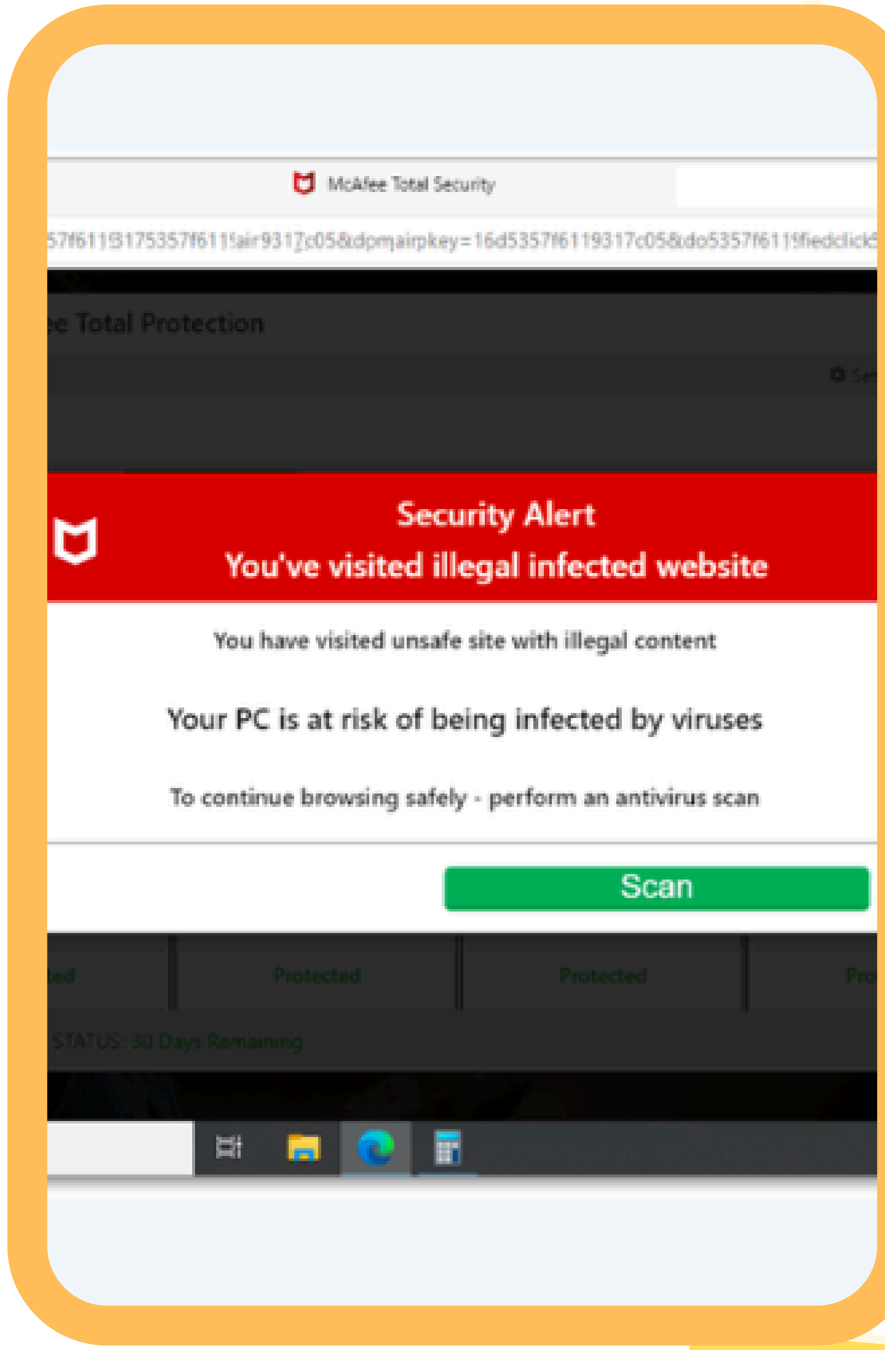
virus have been detected on your iPhone

iOS System Alert

Your iPhone is infected with virus and immediate urgent action is required.

Continue and follow the instructions to fix your iPhone.

Exit at your own risk



McAfee Total Security

57f611f3175357f611!air9317c05&dpmairpkey=16d5357f6119317c05&do5357f611!fiedclick

Security Alert

You've visited illegal infected website

You have visited unsafe site with illegal content

Your PC is at risk of being infected by viruses

To continue browsing safely - perform an antivirus scan

https://veepn.com/blog/fake-virus-warning-popup/

Still anxious?

Sometimes scary ads can leave you anxious, and that is ok! As long as you close out of the ad, you should be fine. If you are still worried, you can go to your anti virus software on your computer or google steps to take to secure your phone or tablet. You can always ask a trusted adult (or tech savvy young person) to help you with this.

Ad Blockers

There are programs out there that you can add to you browser or download to block ads from popping up on websites. These vary by browser. If you want to install one, do your research or have a trusted adult (or tech savvy youth) get this set up for you.

Passwords

Password Management

So many websites require you to make an account. Knowing how to create secure login information and keep track of it is very important. Passwords are meant to keep your information online secure, so don't share your passwords. Pro tip: if you wouldn't trust them with the keys to your house, you shouldn't trust them with your passwords!

Strong Passwords

Strong passwords are

- Long - At least 16 characters
- Random - Mix letters, symbols, and numbers
- Unique - No repeating passwords for different sites
- Contain no personal info - No pet names, old addresses, or DOB

Examples

Some strong password examples include:

- cXmnZK65rf*&DaaD
- Yuc8$RikA34%ZoPPao98t
- Horse Purple Hat Run Bay Lifting
- legal tiny facility freehand probable enamel
- e246gs%mFs#3tv6

Password Managers

Some web browsers will generate and save passwords for you so you don't have to remember them. You can also download a password manager if you want to. Do your research before downloading anything. Of course, you can do it the old fashioned way and write down all your passwords in a dedicated booklet if that suits you best! Just keep it in a safe place you won't forget.

Fake News

FAKE NEWS...

... is often a term quoted by news sources to discredit other news sources. It's best not to believe people shouting this and fact check information for yourself. Online misinformation usually falls into 2 different categories.

Deliberately inaccurate stories – that is, the people publishing them know them to be false but publish them anyway. This might be to manipulate public opinion or to drive traffic to a specific website.

Stories that contain elements of truth but are broadly inaccurate. This might be because the writer hasn't checked all their facts or has exaggerated certain aspects to make a particular point.

Identifying Fake News

Let's walk through some steps to help you sift through all that nonsense on the internet

Check the Source

Check the web address for the page you're looking at. Sometimes, fake news sites may have spelling errors in the URL or use less conventional domain extensions such as ".infonet" or ".offer". If you are unfamiliar with the site, look in the About Us section.

Check the Author

Research them to see if they are credible – for example, are they real, do they have a good reputation, are they writing about their specific area of expertise, and do they have a particular agenda? Consider what the writer's motivation might be.

Check Other Sources

Are other reputable news or media outlets reporting on the story? Are credible sources cited within the story? Professional global news agencies have editorial guidelines and extensive resources for fact-checking, so if they are also reporting the story, that's a good sign.

Maintain a Critical Mindset

A lot of fake news is cleverly written to provoke strong emotional reactions such as fear or anger. Maintain a critical mindset by asking yourself – why has this story been written? Is it promoting a particular cause or agenda? Is it trying to make me click through to another website?

Check the Facts

Credible news stories will include plenty of facts – data, statistics, quotes from experts, and so on. If these are missing, question why. Reports with false information often contain incorrect dates or altered timelines, so it's a good idea to check when the article was published. Is it a current or old news story?

Check the Comments

Even if the article or video is legitimate, the comments below may not be. Often links or comments posted in response to content can be autogenerated by bots or people hired to put our misleading or confusing information.

Check Your Own Biases

We all have biases – could these be influencing the way you respond to the article? Social media can create echo chambers by suggesting stories that match your existing browsing habits, interests, and opinions. The more we read from diverse sources and perspectives, the more likely it is that we can draw accurate conclusions.

Check Whether it's a Joke

Satirical websites are popular, and sometimes it is not always clear whether a story is just a joke or parody. Check the website to see if it's known for satire or creating funny stories. If you want to see some funny fake news, check out the Onion News Network!

Check Images are Authentic

Images you see on social media could have been edited or manipulated. Possible signs include warping – where straight lines in the background now appear wavy – as well as strange shadows, jagged edges, or skin tone that looks too perfect. Bear in mind, too, that an image may be accurate but simply used in a misleading context. You can use tools such as Google's Reverse Image Search to check where an image originates from and whether it has been altered.

Use a Fact Checking Site

Some of the best known include Snopes, PolitiFact, FactCheck, BBC Reality Check

Fake news relies on believers reposting, retweeting, or otherwise sharing false information. If you're not sure whether an article is authentic or not, pause and think before you share.

Social Media

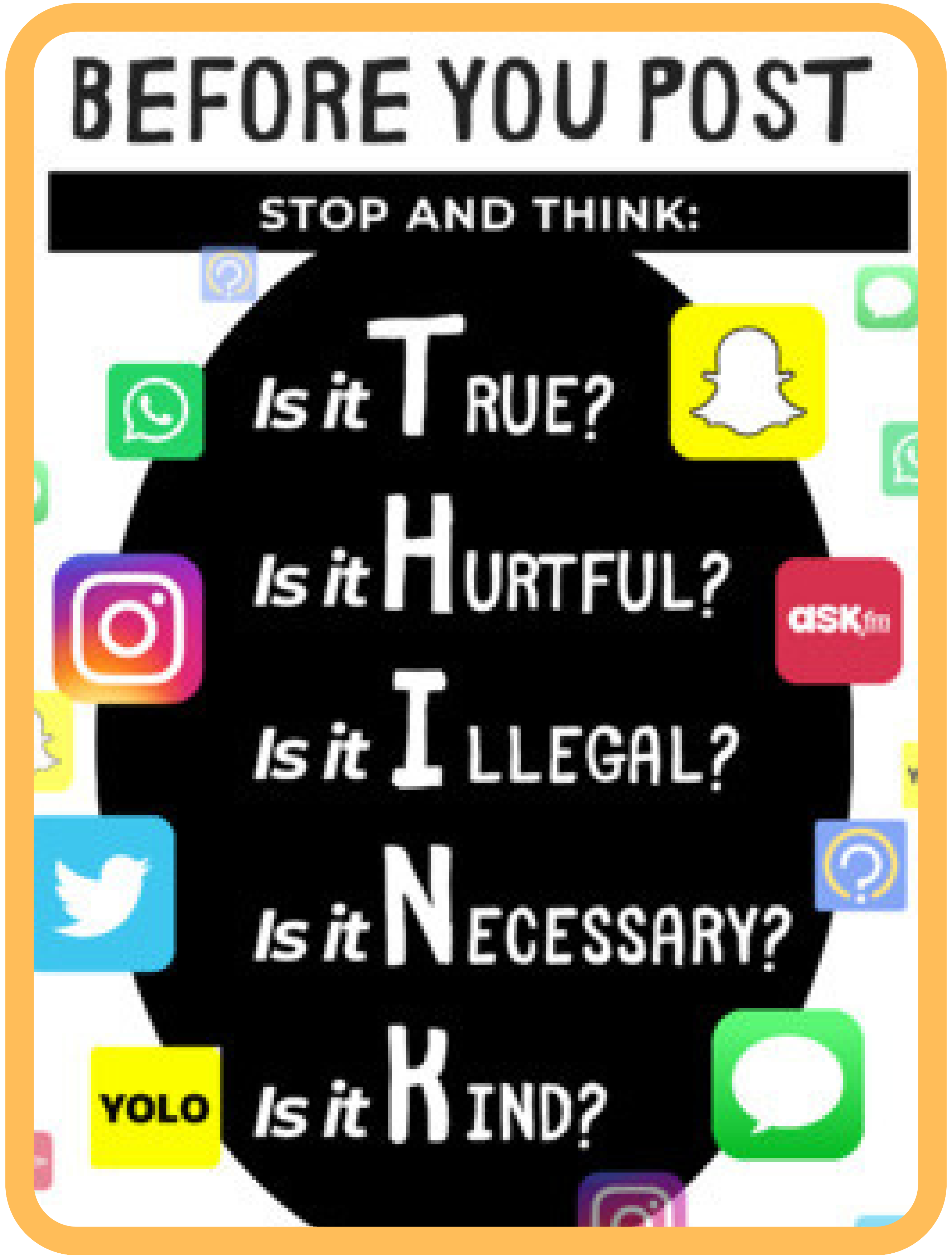
Social Media Safety

Don't Share Person Information

That's the most important thing to remember. Don't share your name, address, phone number, email, location, school, or anything else important online. When in doubt, don't post.

THINK

Let's use social media responsibly and respectfully. THINK before you post!



BEFORE YOU POST

STOP AND THINK:

Is it TRUE?

Is it HURTFUL?

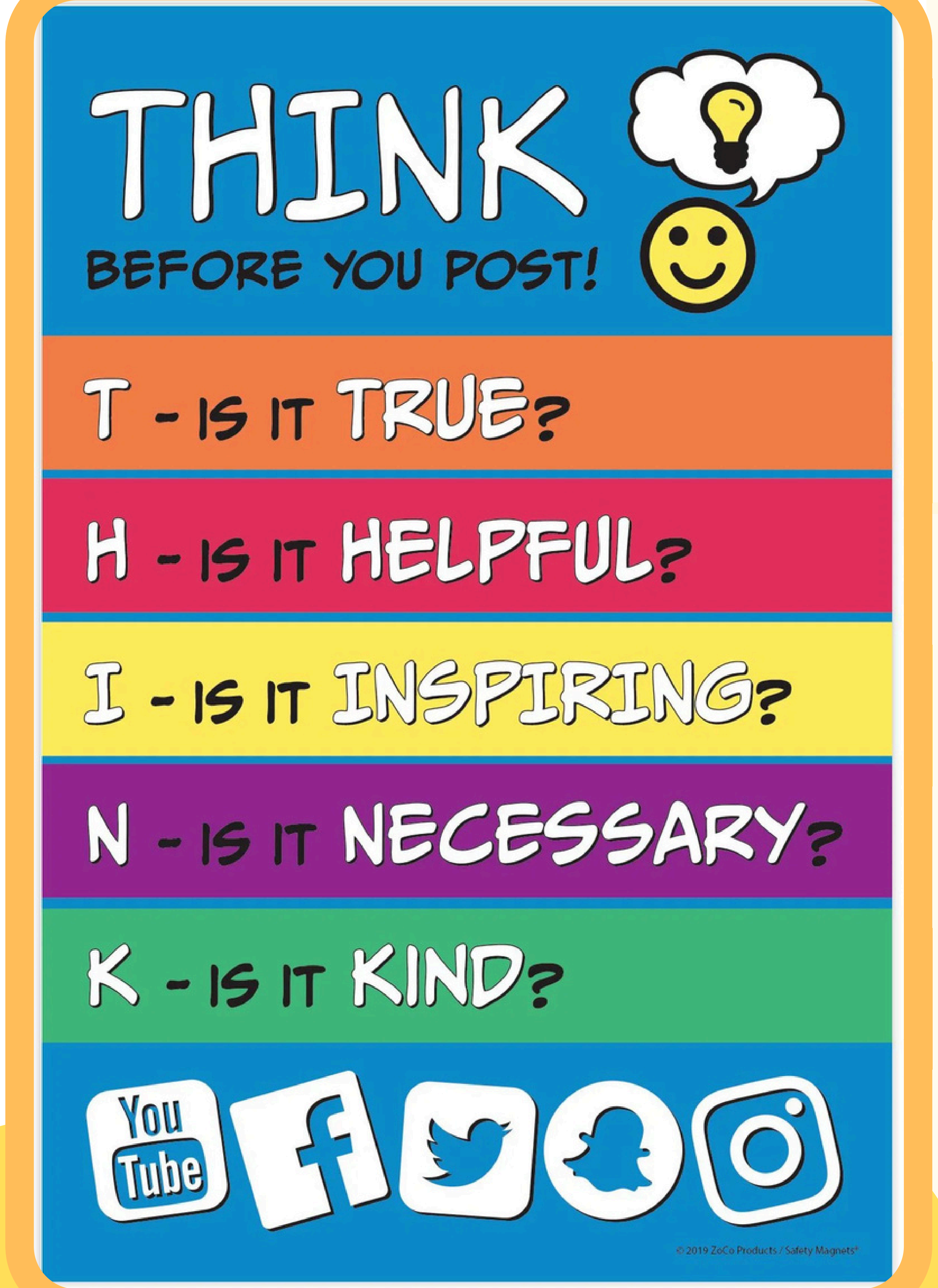
Is it ILLEGAL?

Is it NECESSARY?

Is it KIND?

https://www.teacherspayteachers.com/Product/THINK-Before-You-Post-Posters-with-Icons-4713210

https://www.walmart.com/ip/ZoCo-Think-Before-You-Post-Laminated-12-x18-Multicolor-Classroom-Poster/810187363



THINK BEFORE YOU POST!

T - IS IT TRUE?

H - IS IT HELPFUL?

I - IS IT INSPIRING?

N - IS IT NECESSARY?

K - IS IT KIND?

© 2019 ZoCo Products / Safety Magnets

Posting Online

Everything you share on the internet will permanently exist online!

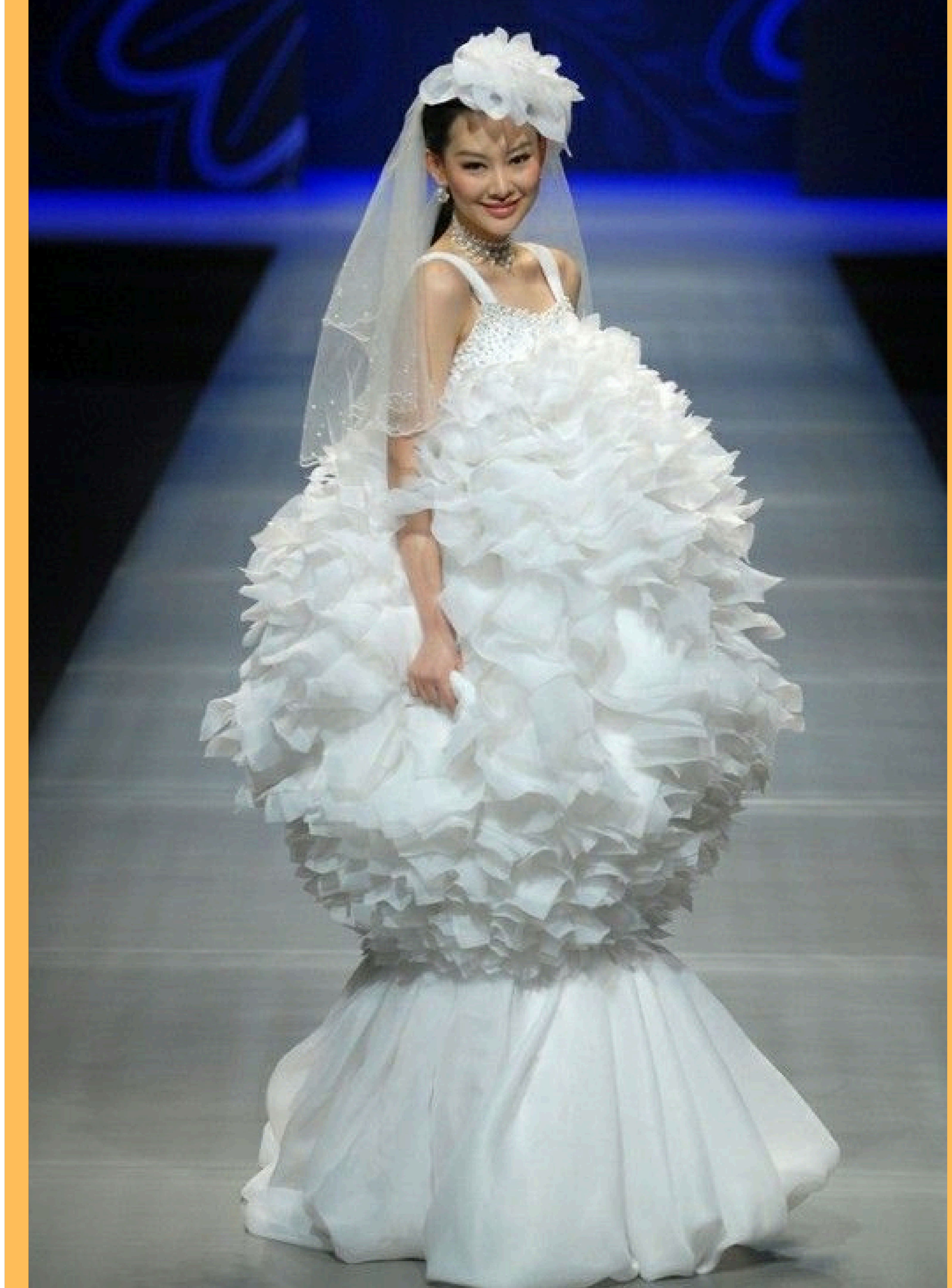
Even if you delete a post, other people could still have it saved, and there are ways people online can recover deleted info. This is why it is imporant to THINK before you post.

Quiz Time!

Your niece has shared photos of her wedding dress online. It is... unique to say the least. The comments are filled with congratulations, as well as remarks about the dress. You see a comment that says "Well isn't that dress just... something else! Bless her heart! Hope the husband is ok with this." Do you:

- Reply agreeing with the commenter
- Reply arguing that the commenter shouldn't be mean considering we all saw what she use to wear back in the 80's
- Comment separately congratulating her and compliment the dress regardless of your personal feelings.
- Don't comment

The Dress In Question



Correct Answer

- Comment separately congratulating her and compliment the dress regardless of your personal feelings.

OR

- Don't comment

Remember: Be NICE!

Quiz Time!

One of your old classmates posts a photo of the house he grew up in. The post details is just a rambling of “remembering the good old days” with a note at the bottom encouraging others to share their memories. You lived right next door to his house and were good friends. Do you...

- Comment “Hey old neighbor! I miss living to your left, we should get coffee sometime and catch up!”
- Post a photo of your old home with the same type of comment.
- Direct message your friend saying “Hey old neighbor! I miss living to your left, we should get coffee sometime and catch up!”
- Don’t comment or post.

Correct Answer

- Direct message your friend saying “Hey old neighbor! I miss living to your left, we should get coffee sometime and catch up!”

OR

- Don’t comment or post.

Remember, we don’t want to share any identifying information publicly. Commenting that you used to live right next to someone who has shared an old address online may open you up to a security breach. Direct messaging them is different, as they already know this information. Sharing an old photo may seem innocent enough, but if your photo has any identifying information (such as a house number) it could be used nefariously.

Tech Help Page!

Thank you for checking out our internet safety presentation. This presentation can be found on our website along with all of our other Nekoosa Help Desk resources.

THANK YOU

Sources

https://usa.kaspersky.com/resource-center/preemptive-safety/how-to-identify-fake-news?srsltid=AfmBOorKQCODmE3swCHrjKug3n3hlLbjDeUXqltRTGbdw_OaGKbtKVoV

https://www.cisa.gov/secure-our-world/use-strong-passwords