Deloitte.

cyber 101

Understanding threats in social media

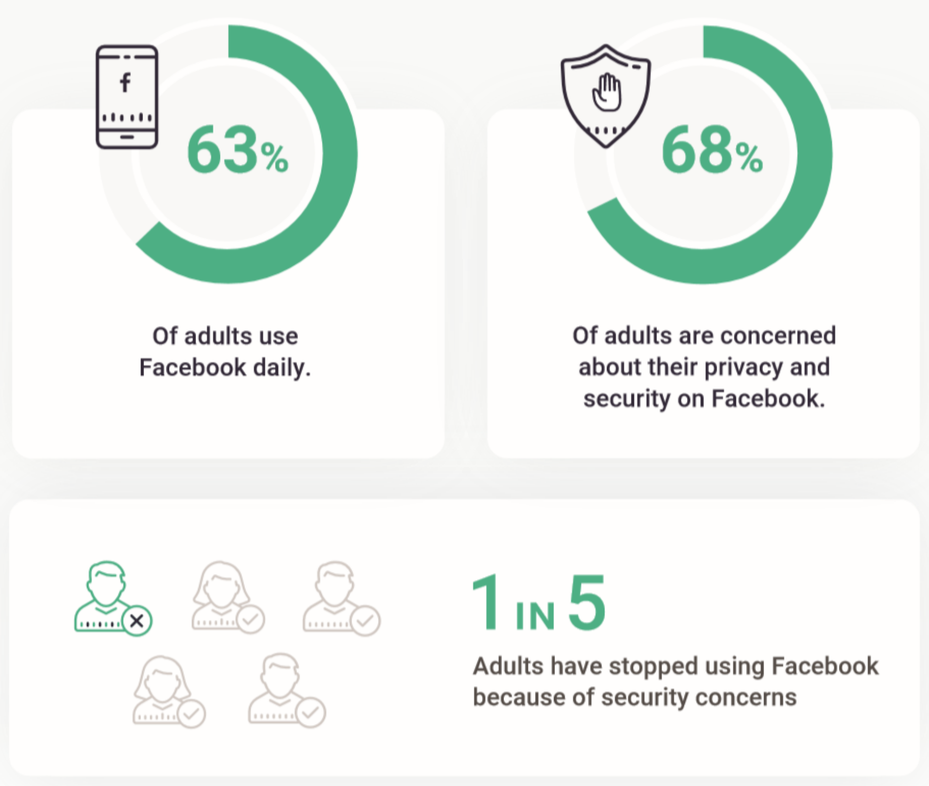
September 2019

Understanding threats in social media

Overview

As we become increasingly connected via digital spaces and share more of our lives and information over social media, we inevitably become more vulnerable to targeted cyber risks.

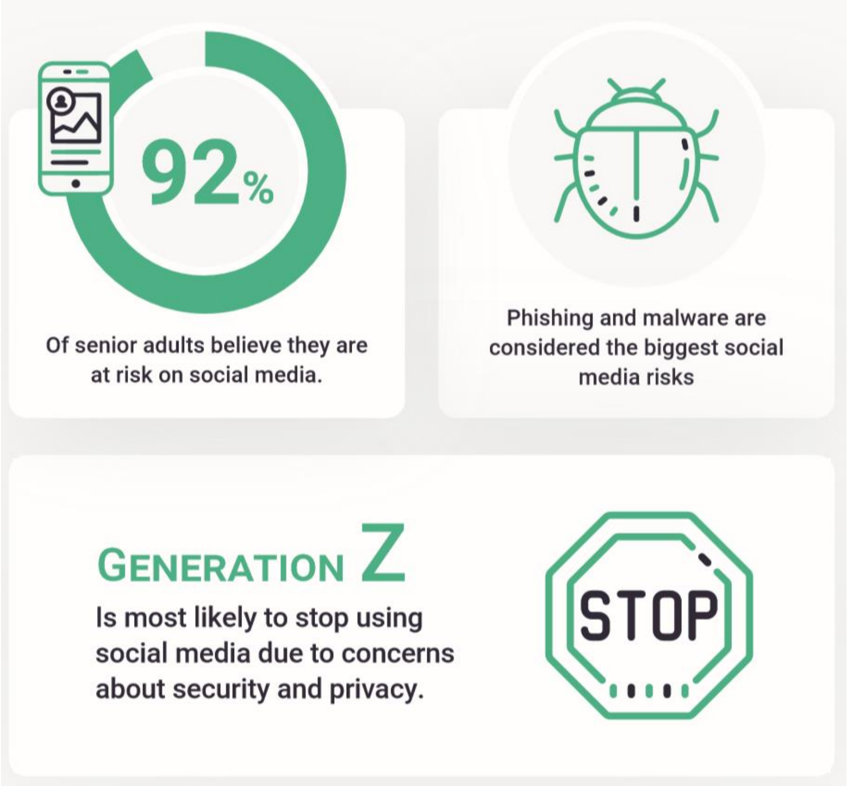
According to the 2019 Study on Social Media Privacy and Security Concerns conducted by ID Experts, majority of adults are using one or more social media platforms at least once per day and are concerned about their security and privacy on social media.



63% Of adults use Facebook daily.

68% Of adults are concerned about their privacy and security on Facebook.

1 IN 5 Adults have stopped using Facebook because of security concerns



92% Of senior adults believe they are at risk on social media.

Phishing and malware are considered the biggest social media risks

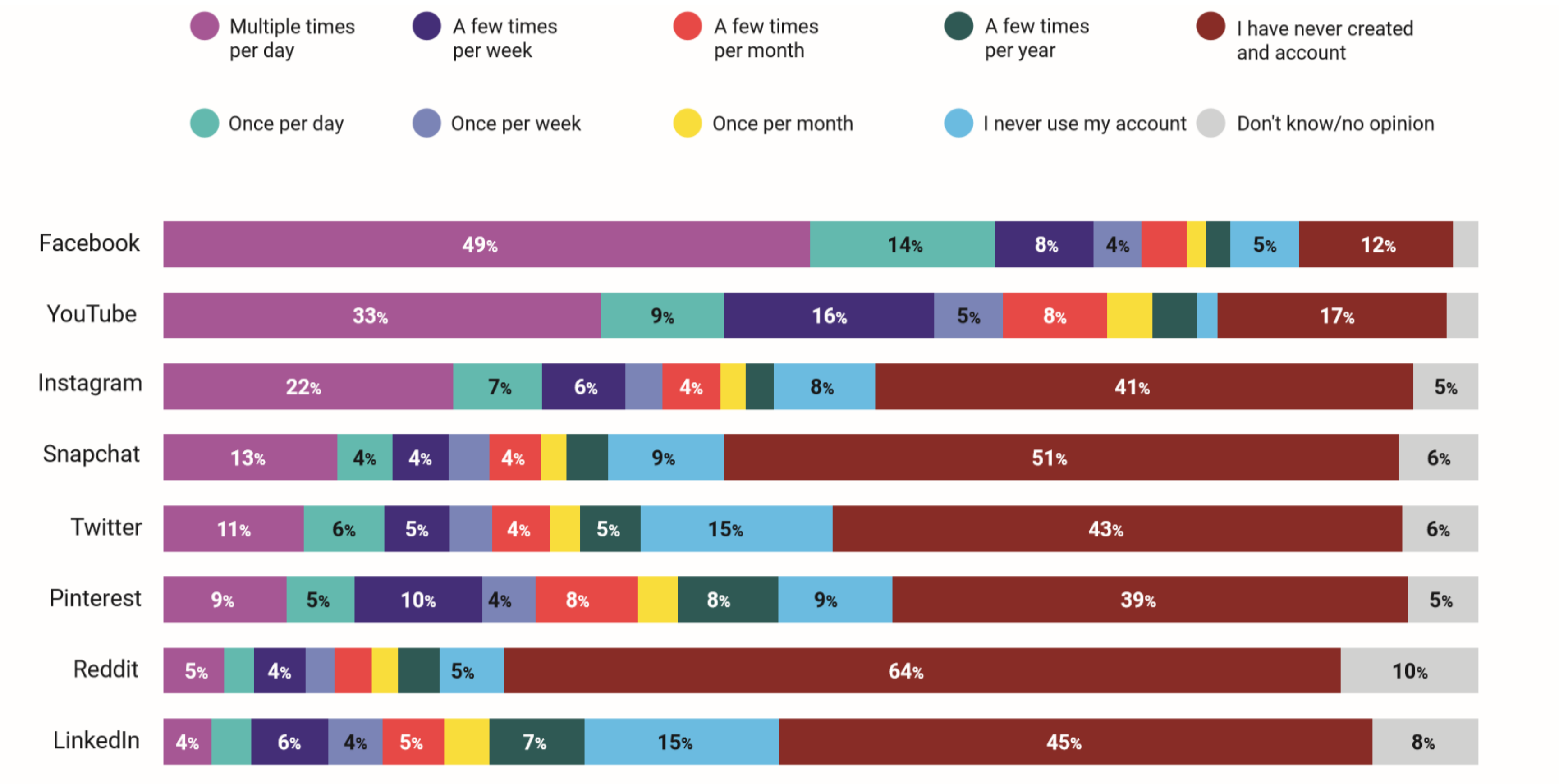
GENERATION Z Is most likely to stop using social media due to concerns about security and privacy.

© 2019 Deloitte & Touche Enterprise Risk Services Pte Ltd

Understanding threats in social media

In-depth look: Social media consumption by platform

Findings indicate that Facebook is the most popular social media platform among adults.



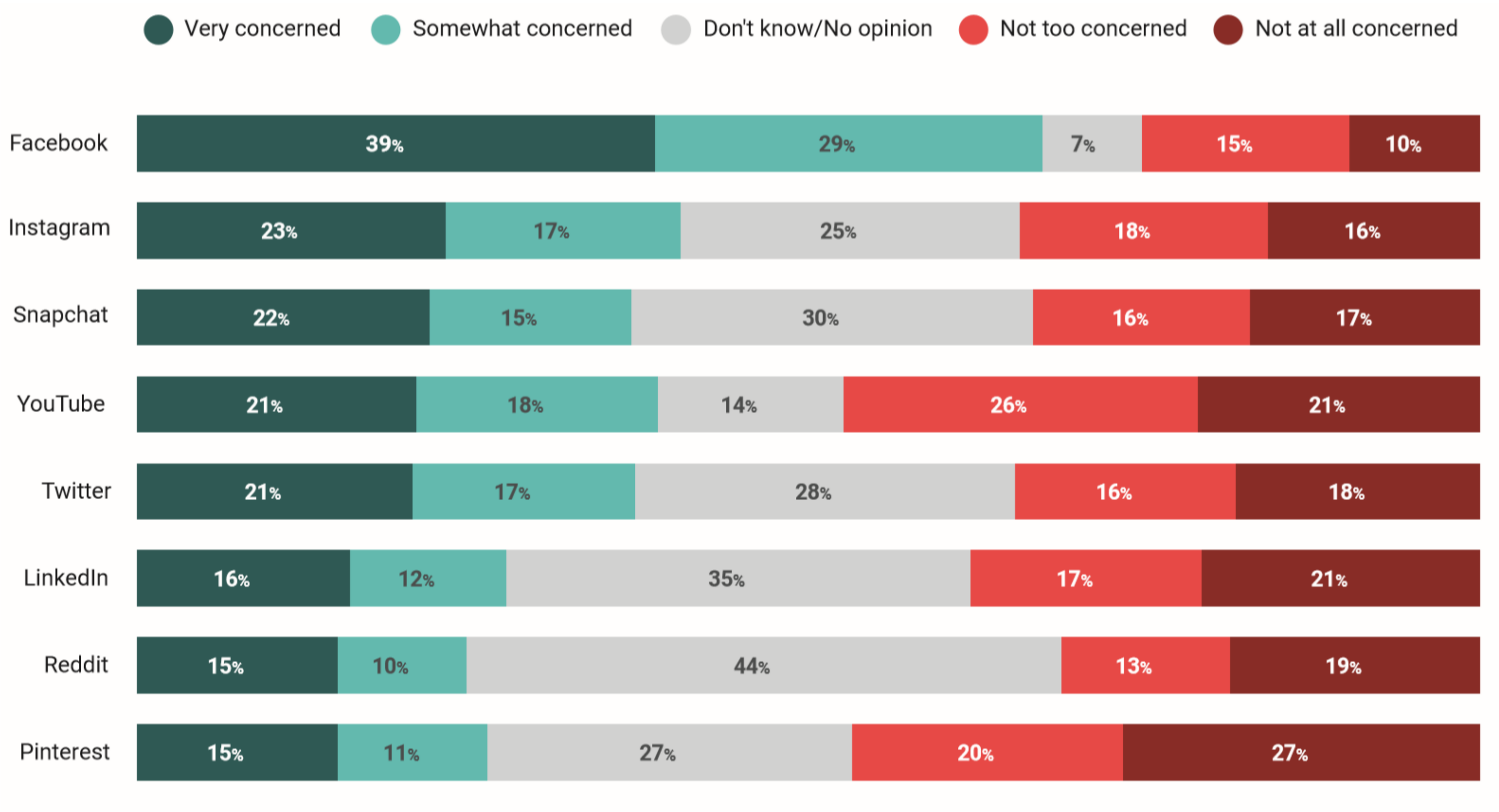
https://www.idexpertscorp.com/knowledge-center/single/2019-study-on-social-media-privacy-and-security-concerns

© 2019 Deloitte & Touche Enterprise Risk Services Pte Ltd

Understanding threats in social media

Survey findings: How concerned are you?

Out of which, 2 in 5 respondents are very concerned about their privacy or security on Facebook.



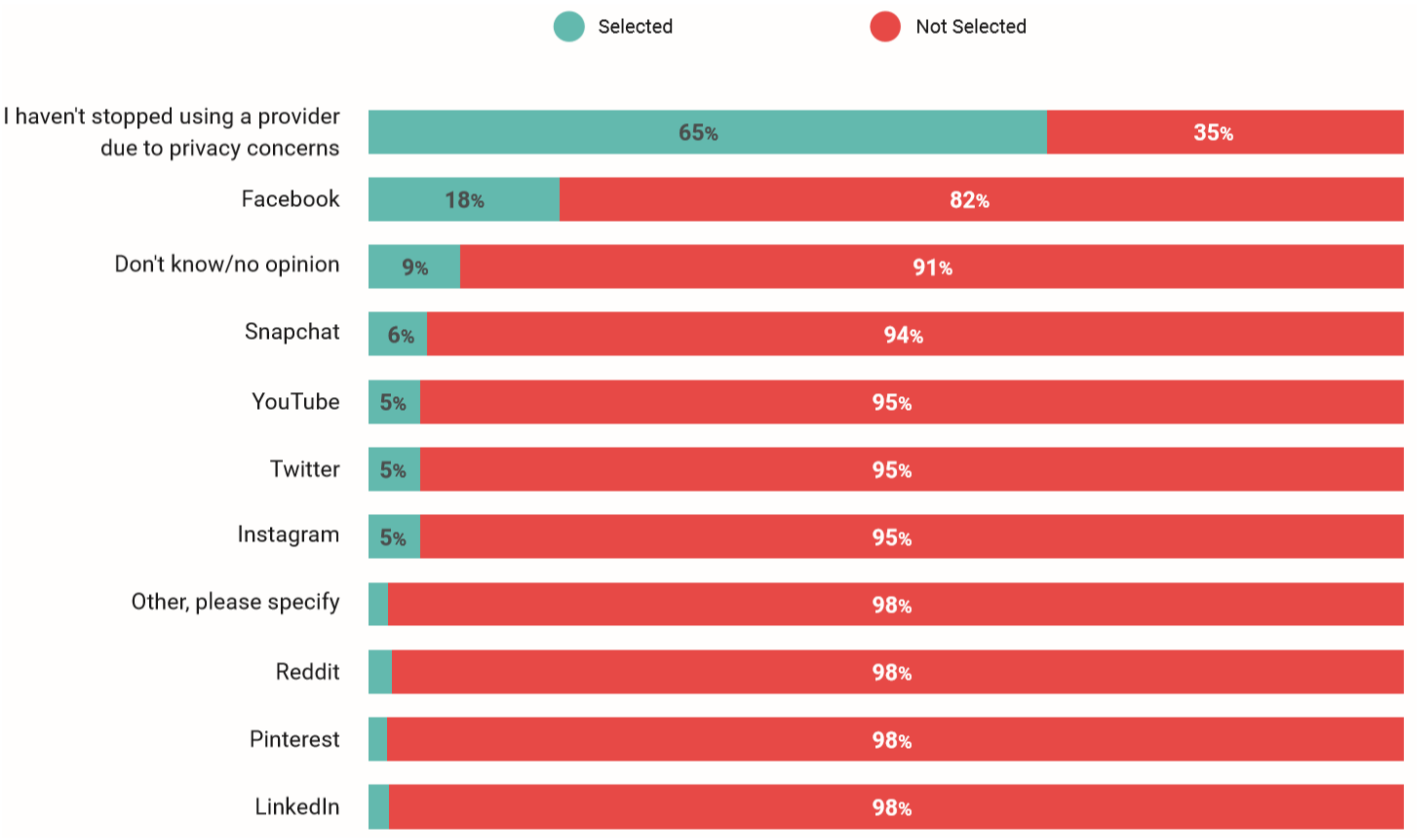
https://www.idexpertscorp.com/knowledge-center/single/2019-study-on-social-media-privacy-and-security-concerns

© 2019 Deloitte & Touche Enterprise Risk Services Pte Ltd

Understanding threats in social media

Survey findings: Termination of social media due to concerns?

1 in 5 respondents have stopped using Facebook as a result of privacy and security concerns.



https://www.idexpertscorp.com/knowledge-center/single/2019-study-on-social-media-privacy-and-security-concerns

© 2019 Deloitte & Touche Enterprise Risk Services Pte Ltd

Understanding threats in social media

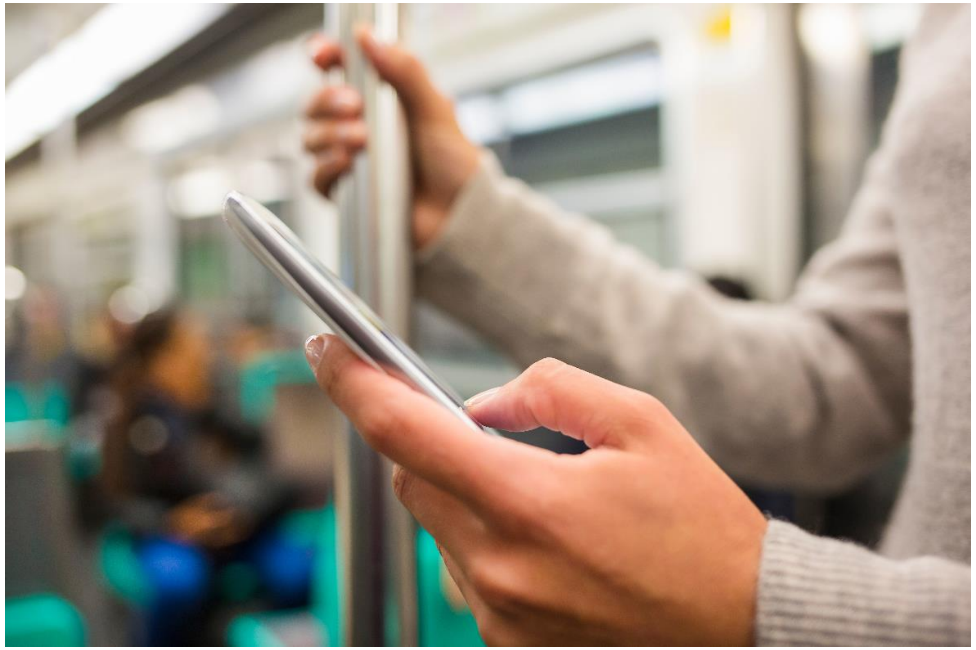
The threats lurking on social media

The fears surrounding privacy and security are not unfounded.

With social media so closely interwoven into our everyday lives, it has become a prime target for cybercrimes and exploitations.

We will explore the four key areas of risks and the ways in which you can protect yourself from them:

1) Data breaches
2) Phishing and malware
3) Catfishing and deception
4) Cyberbullying



© 2019 Deloitte & Touche Enterprise Risk Services Pte Ltd

Understanding threats in social media

1) Data breaches

According to Gemalto's latest Breach Level Index, a global database of public data breaches, social media incidents accounted for over 56% of the 4.5 billion data records compromised worldwide in the first half of 2018.

Here are some well-known cases of data breaches that have occurred in social media giants:

Facebook's code vulnerability affected 50 million users, potentially exposing personal information and enabling hackers to take control of user profiles. (Source)

Google+ shuts down following a glitch through which external developers were able to access the data of over 500,000 users. (Source)

Instagram breach exposes personal contact information of 350,000 influencers. (Source)

How to protect yourself?

- While such attacks are beyond users' control, turning on **two-factor authentication** limits your exposure. Even if someone has your password, they cannot access your account without a unique code verification sent by a text, call or email.
- Conduct a **device audit** once you know of a breach, and remove devices you do not recognise from being logged in to your account.

© 2019 Deloitte & Touche Enterprise Risk Services Pte Ltd

Understanding threats in social media

2) Phishing and malware

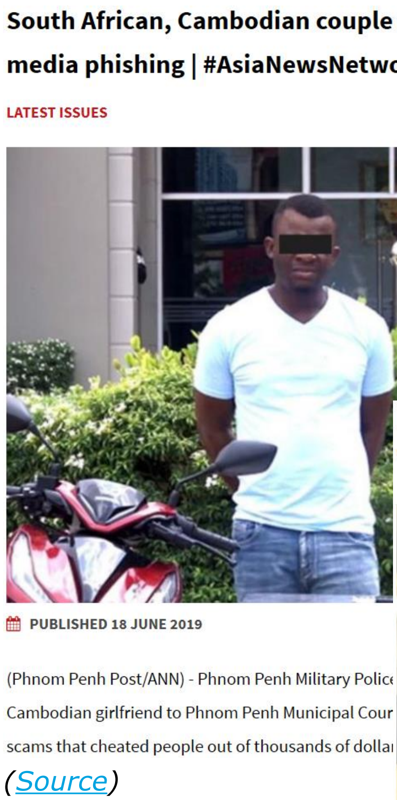
Phishing occurs when cyber criminals employ social engineering techniques to trick users into clicking deceptive links to download malware (short for malicious software).

On social media, such deceptive links often appear in the form of unbelievable news, giveaways and shocking videos.

Cyber criminals may also design games and quizzes to trick users into entering their personal information, subscribing them to unwanted services that would appear in their phone or credit card bills.

How to protect yourself?

- Always be **cautious** when clicking on links and attachments. Look out for spelling errors and URLs that do not seem legitimate.
- Use a **security software** that can stop malware from being installed on your computer.



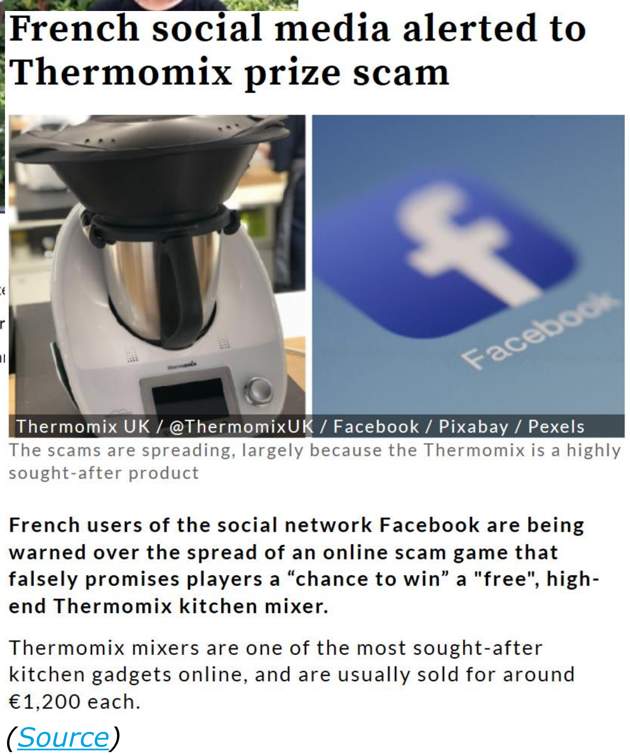
South African, Cambodian couple apprehended for social media phishing | #AsiaNewsNetwork

LATEST ISSUES

PUBLISHED 18 JUNE 2019

(Phnom Penh Post/ANN) - Phnom Penh Military Police Cambodian girlfriend to Phnom Penh Municipal Cour scams that cheated people out of thousands of dolla

(Source)



French social media alerted to Thermomix prize scam

Thermomix UK / @ThermomixUK / Facebook / Pixabay / Pexels

The scams are spreading, largely because the Thermomix is a highly sought-after product

French users of the social network Facebook are being warned over the spread of an online scam game that falsely promises players a “chance to win” a "free", high-end Thermomix kitchen mixer.

Thermomix mixers are one of the most sought-after kitchen gadgets online, and are usually sold for around €1,200 each.

(Source)

https://uk.norton.com/internetsecurity-online-scams-11-social-media-threats-and-scams-to-watch-out-for.html

https://us.norton.com/internetsecurity-malware-5-ways-you-didnt-know-you-could-get-a-virus-malware-or-your-social-account-hacked.html

© 2019 Deloitte & Touche Enterprise Risk Services Pte Ltd

Understanding threats in social media

3) Catfishing and deception

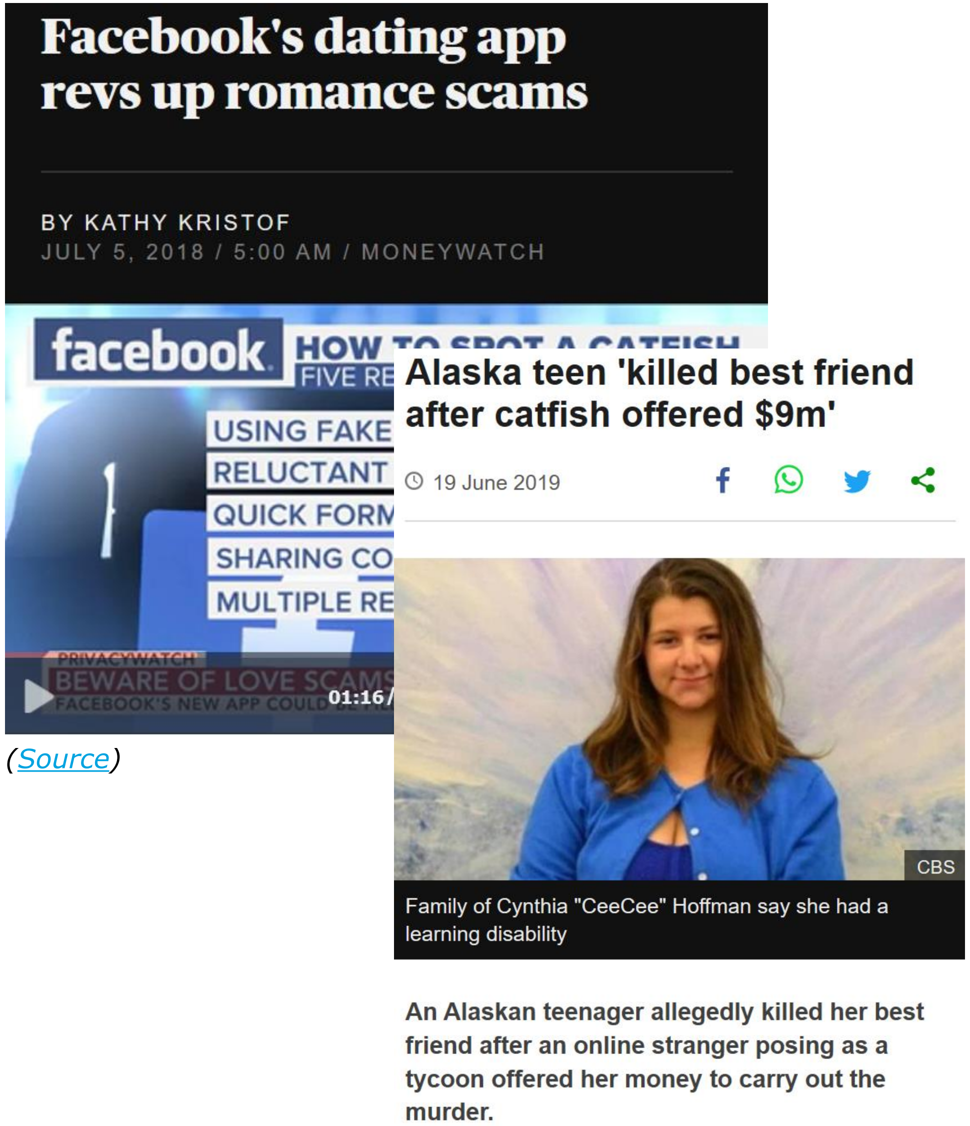
Catfishing is a term used to describe someone who purposefully deceives others online by impersonating as someone else or creating an identity that does not portray their actual self. This may involve fake names, stolen or edited photos, made up identities, or false experiences to deceive others.

While some catfish may use their false identity to solicit money from their victims, the motivations for catfishing are often emotional. They include loneliness, personal insecurities, boredom, mental illness, revenge, harassment and others.

In a survey conducted by phys.org, loneliness was cited by 41% of respondents as the reason for their catfishing.

Although catfishing is not a crime, the implications for individuals who have been catfished can be extremely damaging to their mental health and result in embarrassment.

Avoiding getting catfished is increasingly difficult, especially as online dating is becoming commonplace. Therefore, it is imperative to **verify the identity** of individuals to avoid getting misled.



Facebook's dating app revs up romance scams

BY KATHY KRISTOF
JULY 5, 2018 / 5:00 AM / MONEYWATCH

(Source)

Alaska teen 'killed best friend after catfish offered $9m'

19 June 2019

Family of Cynthia "CeeCee" Hoffman say she had a learning disability

An Alaskan teenager allegedly killed her best friend after an online stranger posing as a tycoon offered her money to carry out the murder.

(Source)

https://phys.org/news/2018-07-catfish-people-onlineit-money.html

https://www.cybersmile.org/what-we-do/advice-help/catfishing

© 2019 Deloitte & Touche Enterprise Risk Services Pte Ltd

Understanding threats in social media

4) Cyberbullying

According to a survey by CNA, 3 in 4 children and teenagers in Singapore have been a victim of cyberbullying.

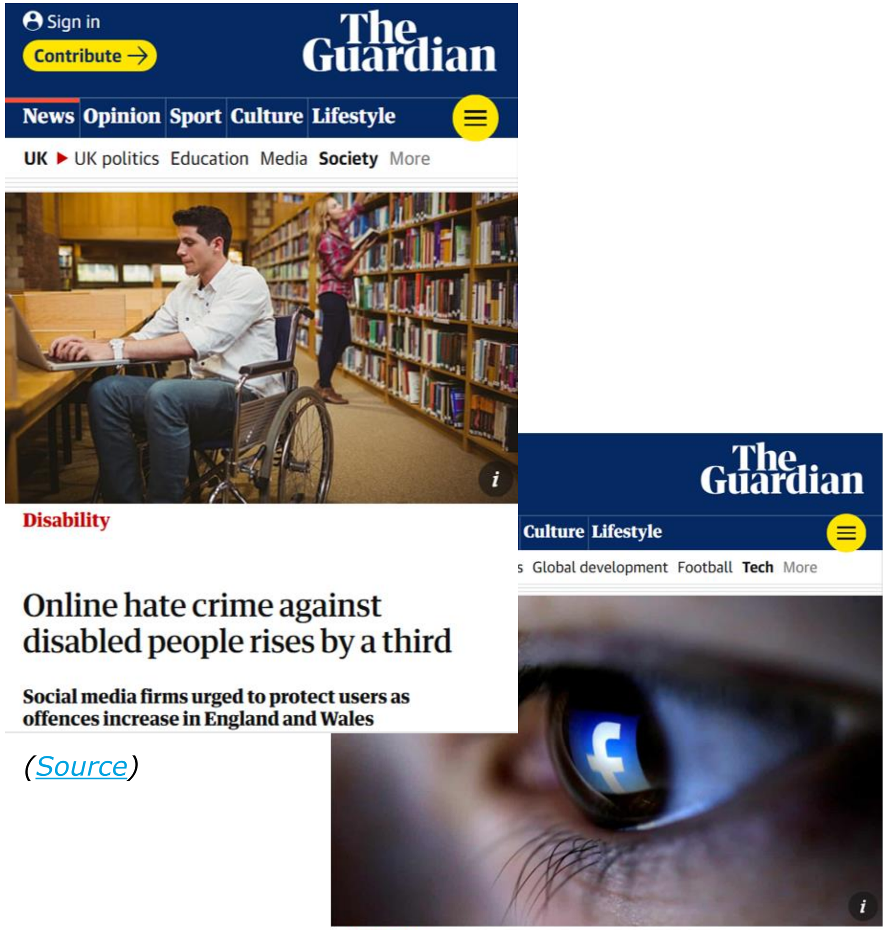
Cyberbullying is abuse that takes place over digital platforms such as online social media sites, messenger apps, forums, and other platforms where people can view, participate and share content.

It includes sharing, sending or posting of negative, harmful, mean or false content aimed at harming or humiliating another individual. Cyberbullying affects individuals in the digital space, but can also have direct impact to the physical, mental and emotional safety of individuals offline.

How to protect yourself?

Take steps to address cyberbullying when it escalates beyond minor teasing and name-calling.

- Save the evidence
- Block the bully
- Report the bully to the web administrator
- If there are threats of physical harm, report it to the authorities such as the police.


Sign in
Contribute →
The Guardian
News Opinion Sport Culture Lifestyle
UK ▶ UK politics Education Media Society More
The Guardian
Culture Lifestyle
s Global development Football Tech More

Disability

Online hate crime against disabled people rises by a third

Social media firms urged to protect users as offences increase in England and Wales

(*Source*)

Facebook

Facebook criticised after women complain of inaction over abuse

Amnesty says social media firm must do more to support users who report harassment

(*Source*)

https://www.stopbullying.gov/cyberbullying/what-is-it/index.html
https://onlinesense.org/how-to-protect-yourself-from-cyberbullies/

© 2019 Deloitte & Touche Enterprise Risk Services Pte Ltd

Understanding threats in social media

Protect yourself

cyber 101

As cybercriminals and individuals with malicious intent constantly evolve to exploit users, here are a few rules of thumb you should follow to remain vigilant and secure:

Use strong passwords. A strong password helps to protect your account against hackers.

Be selective with friend requests. Verify their identity to ensure it is not a fake account.

Be mindful of what you share. Avoid sharing personal or sensitive information.

Click links with caution. Look out for language and content that is suspicious or too good to be true.

Protect your computer with antivirus software. Frequent PC updates helps to protect against malware.

Be aware of your privacy settings. Change your privacy settings to control who can see your content.

https://www.getcybersafe.gc.ca/cnt/rsks/nln-ctvts/scl-ntwrkng-en.aspx

© 2019 Deloitte & Touche Enterprise Risk Services Pte Ltd

Deloitte.

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited ("DTTL"), its global network of member firms, and their related entities. DTTL (also referred to as "Deloitte Global") and each of its member firms and their affiliated entities are legally separate and independent entities. DTTL does not provide services to clients. Please see www.deloitte.com/about to learn more.

Deloitte is a leading global provider of audit and assurance, consulting, financial advisory, risk advisory, tax and related services. Our network of member firms in more than 150 countries and territories serves four out of five Fortune Global 500® companies. Learn how Deloitte's approximately 286,000 people make an impact that matters at www.deloitte.com.

Deloitte Asia Pacific Limited is a company limited by guarantee and a member firm of DTTL. Members of Deloitte Asia Pacific Limited and their related entities provide services in Australia, Brunei Darussalam, Cambodia, East Timor, Federated States of Micronesia, Guam, Indonesia, Japan, Laos, Malaysia, Mongolia, Myanmar, New Zealand, Palau, Papua New Guinea, Singapore, Thailand, The Marshall Islands, The Northern Mariana Islands, The People's Republic of China (incl. Hong Kong SAR and Macau SAR), The Philippines and Vietnam. In each of these, operations are conducted by separate and independent legal entities.

About Deloitte Singapore
In Singapore, services are provided by Deloitte & Touche LLP and its subsidiaries and affiliates.

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited, its member firms, or their related entities (collectively, the "Deloitte Network") is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser. No entity in the Deloitte Network shall be responsible for any loss whatsoever sustained by any person who relies on this communication.

© 2019 Deloitte & Touche Enterprise Risk Services Pte Ltd