Online Safety

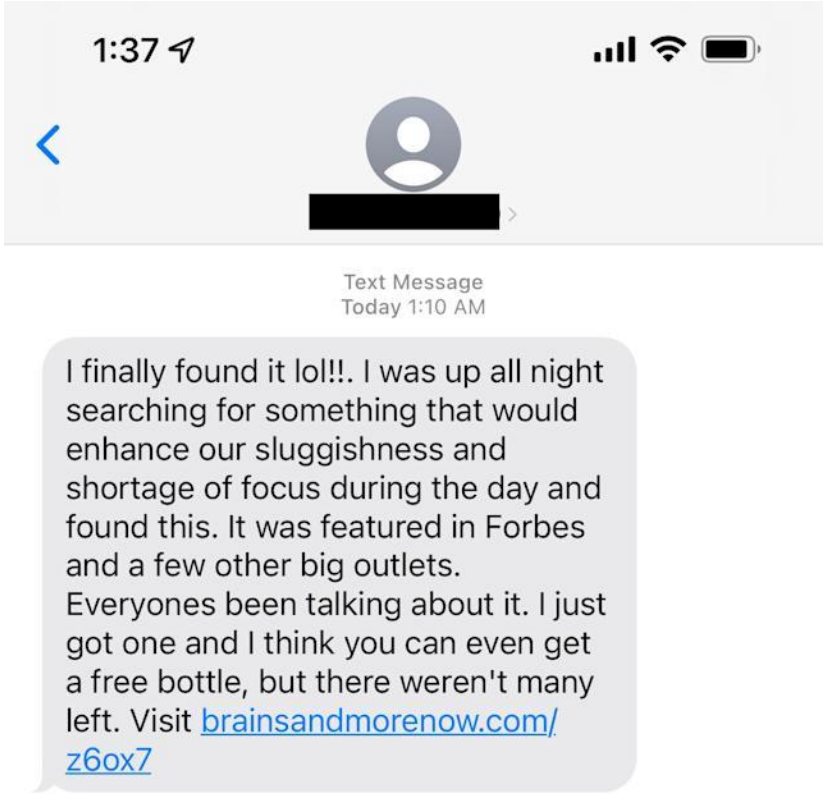
By: Isaac Chang

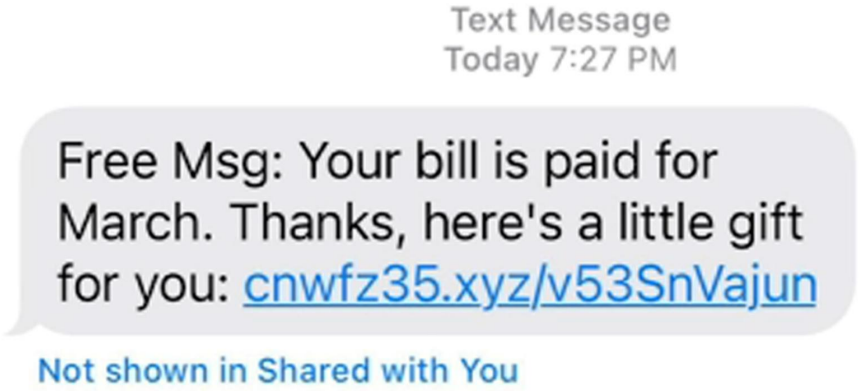
Do you use these online applications?

1. Text messaging (iMessage, WhatsApp, Facebook, WeChat, etc.)
2. Watch videos online (YouTube, TikTok, Instagram)
3. Social networking (Facebook/Meta, Instagram,etc.)
4. Mobile phone

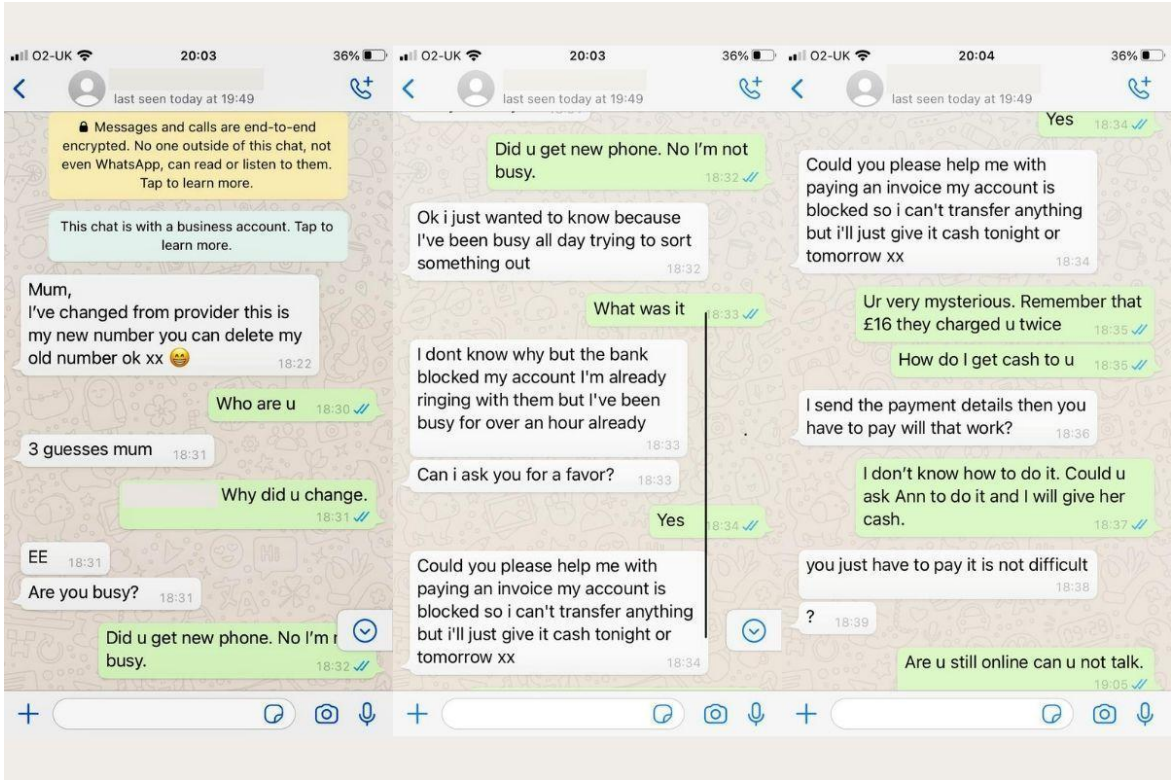
If you do, you are the potential target of cyber criminals.

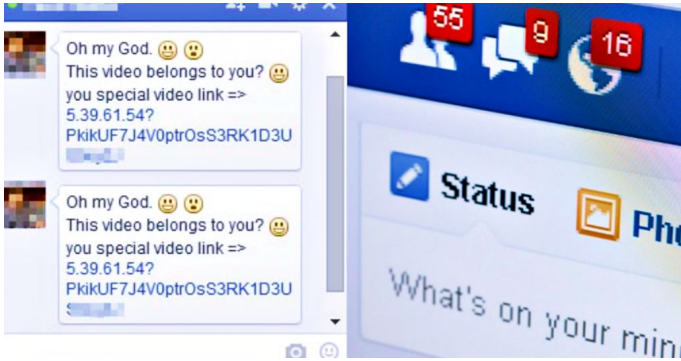
Examples of spam text messages & calls



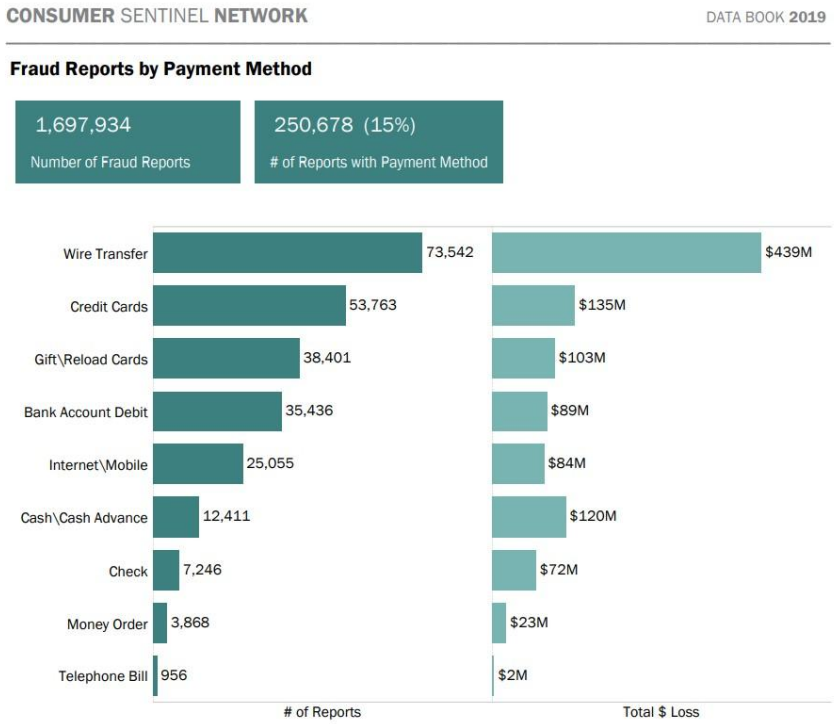


Examples of Facebook & WhatsApp hacks

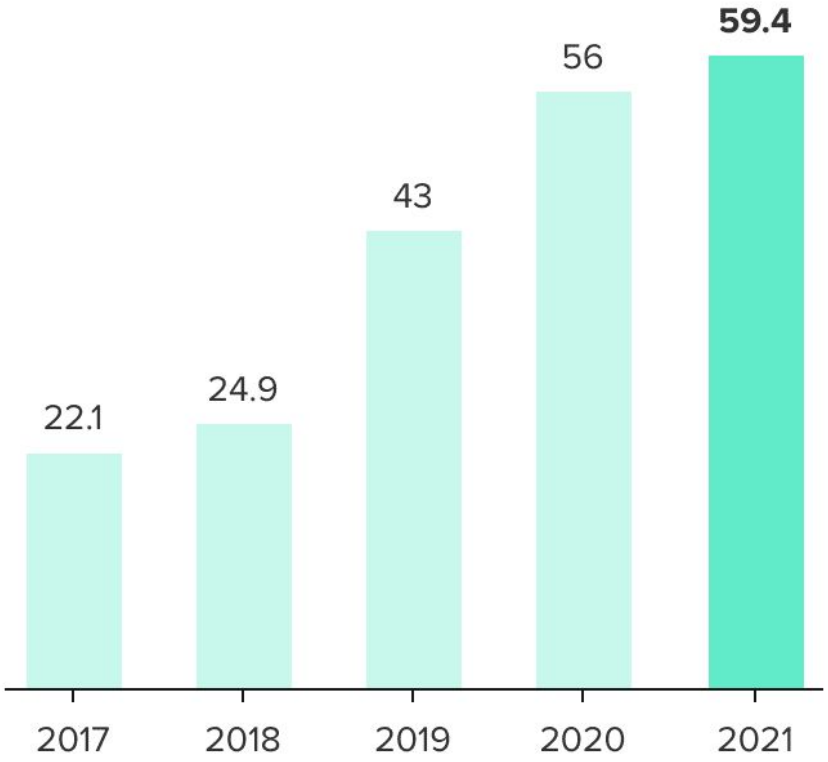




Why should you care about online safety?



Total Americans who lost money to scam calls (in millions)



Source: Truecaller

CNBC make it

Tips to protect yourself from scams

1. Information (email address, phone #, etc) of sender doesn't match what they are saying
2. Government organizations like the IRS will NOT call you and demand payment
3. What online strangers are saying don't match up with what you have done
4. Questionable payment methods (asking for gift cards from the local store)
5. Ridiculous backstories (i.e. some foreign country royalty offering money in return for bank information)
6. Text messages telling you that you won a lottery ticket
7. Phone calls from organizations pretending to be big companies demanding money
8. Anyone asking for your personal information

The structure of scams:

1. Fear - things that will make people feel intimidated
2. Urgency - things need to happen right now
3. Gift - "too good to be true"

Hands on learning: How to spot spam emails

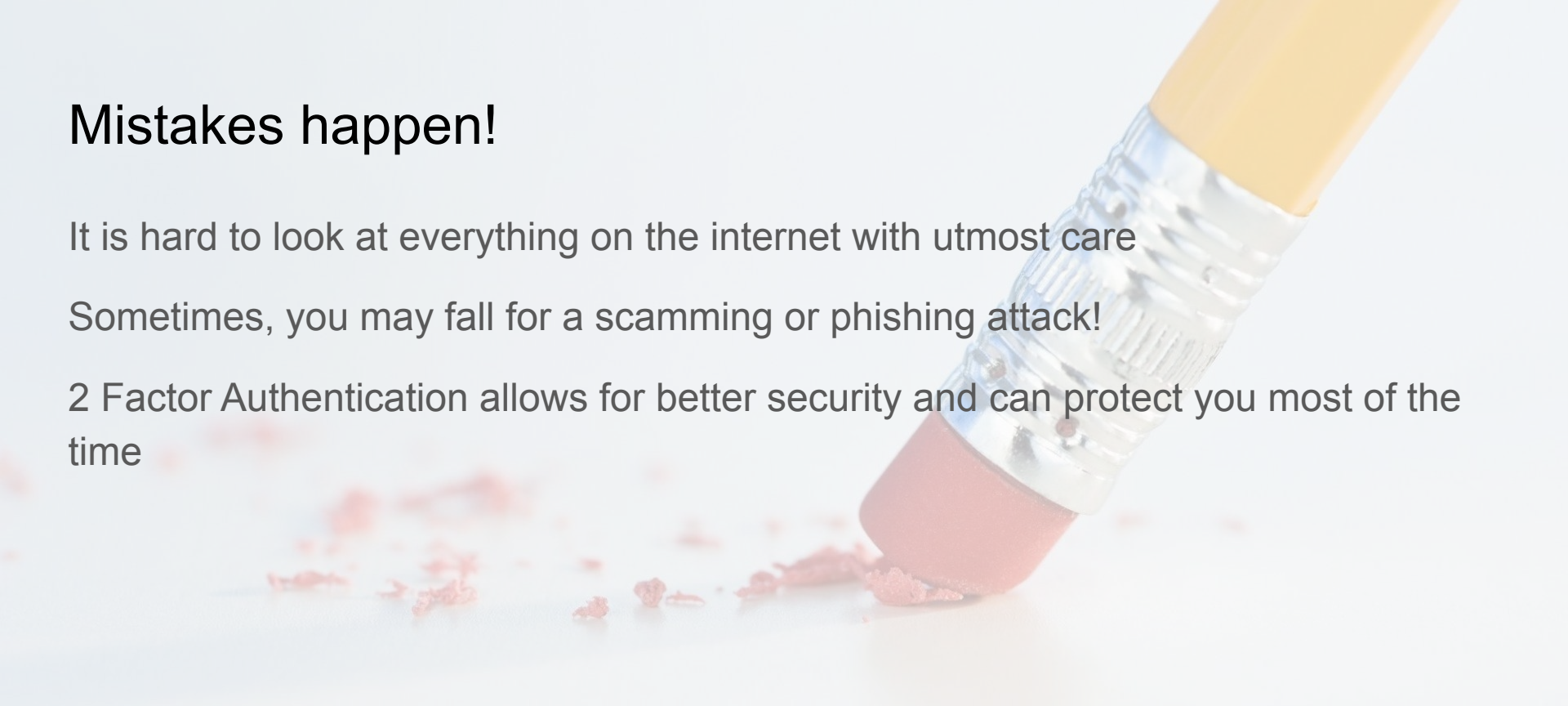
https://phishingquiz.withgoogle.com/

Mistakes happen!

It is hard to look at everything on the internet with utmost care

Sometimes, you may fall for a scamming or phishing attack!

2 Factor Authentication allows for better security and can protect you most of the time



Conclusion

Top 3 things to remember:

1. Look for threats or “too good to be true” feelings
2. Double check what the sender wants you to do
3. Stay calm no matter how threatening the conversation/message/email may be

Thanks for listening