**Kahoots**

1. The top method for scammers to target consumers is:

A. Direct mail C. phone calls and text messaging

B. E-mails D. None

2. The Top Fraud of 2020 Goes to:

A. Imposter scams C. Ghosting Scams

B. Keylogger scams D. Phishing scams

3. Imposter scams includes scammers who:

A. Act as government officials stealing stimulus payments.

B.  Pretend to be healthcare workers in COVID-19 testing and [vaccine scams](https://idtheftcenter.us19.list-manage.com/track/click?u=fba66e1a225eda5e30bd00da9&id=c5280db90b&e=59baeca76d)

C. Fake charity scams

D. All of the above

4. Which of these organizations would NOT be an agency you can go to for help, if scammed?

A. FTC - Federal Trade Commission ([www.ftc.gov](http://www.ftc.gov))

B. Identity Theft Resource Center (<https://www.idtheftcenter.org/>)

C. U.S. Department of Justice, Office of Victims of Crime (<https://ovc.ojp.gov/>)

D. HugeDomains.Com ([www.iwishgoods.com](http://www.iwishgoods.com))

5. Scammers pretending to be interested in you, asking for your e-mail and later ask for financial help to come visit you. This is a:

A. Dating scam C. Phishing scam

B. Ghosting scam D. Skimming scam

6. You receive a phone call claiming you won a prize but require a fee to collect it and/or e-mail, address or phone to contact you. This is a:

A. Sweepstake scam C. Man-in-the Middle scam

B. Ghosting scam D. Pharming scam

7. You are sent a counterfeit check that looks real. Scammer tells you to deposit the check but asks you to ”refund” a portion as they have sent you too much money. This is a:

A. Charity scam C. Phishing scam

B. Banking scam D. Pharming scam

8. A scammer sets up a fake organization, especially after disasters. They ask you to contribute to their fund sounds similar to other well-known organizations.

A. Charity scam C. Phishing scam

B. Banking scam D. Pharming scam.

9. Outside the Super Bowl, scammers are selling seats which have a barcode and legitimate logos for the event. All they ask is for a credit card number for the seat.

A. Ghosting scam C. Phishing scam

B. Rogue scam D. Ticketing scam

10. Hackers from foreign countries have been hacking into U.S. government offices, corporations, hospitals and banks. This is a:

A. Brute Force scam C. Spoofing scam

B. Hash Buster scam D. Vishing scam

11. Someone who creates a fake online profile to intentionally deceive you is a:

A. Ghost scammer C. Phishing scammer

B. Catfish scammer D. Hash Buster

12. The random words or sentences contained in spam e-mails that allow these e-mails to bypass your spam filters.

A. Ghost scammer C. Phishing scammer

B. Catfish scammer D. Hash Buster

13. Malicious online advertising that contains software intended to damage or disable computers is referred to as.

A. Malware C. Spyware

B. Whaling D. Scareware

14. When hackers use malicious programs to route you to their websites, even if you’ve correctly

typed in the address of that site you want to visit. This is referred to as:

A. Phishing C. Pharming

B. Ransomware D. Scareware

15. The act of trying to trick you, into providing sensitive personal data or credit accounts by a scammer posing as a trusted business or other entity. This is referred to as: A. Phishing C. Pharming

B. Ransomware D. Scareware