What does some of the data show about online scammers, how pervasive is this?

Key Stats:

- According to Javelin Strategy & Research, in 2021, 915,000 children - 1 in 80 - were the target of identity theft and 1 in 43 children were affected by data breaches
- From 2017-2021, victims under 20 have seen a 1126% increase in money lost to online scams, marking the highest increase of any age group over the five-year period according to the FBI IC3
- The FBI received 15,782 reports of online/digital scams from people age 19 and younger in 2022, with losses of $210.5 million (more than double 2021's reported losses)

Note 1: Motivations include: financial, predatorial, exploitation, fraud, etc.

What are the most common types of online scams, focusing a bit more on holidays?

1. **Fake charities** - scammers create "lookalike" sites or campaigns to take advantage of people's generosity during the holidays
2. **Scam products on social media** - scammers create ads on TikTok, Instagram, or X (formerly Twitter) that offer products that are either never shipped once paid for, or are completely different from what's been advertised.
    - Also, some ads on social media can even lead to fake online stores that mimic real brands in order to trick people into giving their personal and financial information, or force you to use a third-party payment that cannot be reversed (Zelle, wire transfer, etc.)
3. **Fake online giveaways and surveys on social media** - scammers promote these false giveaways or create surveys that have fake prizes, like free money, in exchange for personal information
4. **Fake delivery notifications** - scammers send a text saying that a package has failed to deliver. The text will contain a link that sends the person to a bogus site that's designed to your steal information or fool you into giving them money

5. **Exploitation** - scammers will manipulate victims using a proxy victim motivated by financial concerns in order to target relationships of the proxy thus creating a scaled exploitation model.

Note 2: Catfishing (fake persona) sextortion, Social media, College admission/scholarship, Identity theft

How are children targeted (specific to scams)? In particular, how does social media exacerbate this?

While kids today do have the skills to navigate the internet safely, internet scammers have become increasingly sophisticated at taking advantage of children online. They adapt their tactics to seem harmless amidst normal internet behaviors. So, children may not realize the potential consequences of their actions. Social media has increased the number of opportunities for scammers to connect with kids, since social platforms make interacting with strangers a normal occurrence. While posting details about their school, activities, or home life may be second nature for children, this information allows scammers to more easily commit fraud using their identities.

Types of popular social platforms scams can be found on:

1. **Videos** - Popular sites like YouTube, Snapchat, Instagram, Twitch.tv and TikTok create opportunities for scammers to reach kids through messaging or embedded links, and encourage them to share personal information.

Example scenarios:

- Incorporate quizzes to “learn who has a crush on you” or other clickbait messages to lure kids into giving personal information
- Have ads that lead to sites or online stores that are fake

2. **Gaming platforms** - Desktop computers and gaming consoles such as Xbox, Switch and PS5 have private messaging capabilities, screen sharing, or allow users to speak to each other with a microphone that scammers can take advantage of.

Example scenarios:

- Scammers can send a message with a link leading to a third-party messaging app saying that they want to “team-up

or create a party" where they'll then try to gain personal information disguised as an attempt to "make friends"
- Some can even pose as kids using voice modulating or cloning technology which scammers use to build trust with a kid over a period of time. The kid would feel more comfortable sharing personal information with their "friend"

3. **Rideshare** - In exploitation situations, proxy children motivated by financial gain or other incentives will use ride shares to move victims around for exploitation.

What are actionable tips for parents to keep themself and their children safe from scammers?

- Look at real-world examples of potential scams together and evaluate them together
- Start by establishing boundaries, acceptable behaviors and guidelines for device use
- Inform them what key information to avoid sharing online (such as where they go to school, what their parents do for work, driver license numbers, etc.)

How should parents talk to their kids about this?

- Discuss without judgment
- Instill critical thinking about what they see
- Empower them to ask questions if unsure
- Let them know you're there to protect them
- Set "guardrails" with guidance.

References:

https://www.aura.com/learn/holiday-scams

https://www.onpointcu.com/blog/how-scammers-target-kids-online/

https://www.aarp.org/money/scams-fraud/info-2022/child-identity-theft.html

https://socialcatfish.com/scamfish/state-of-internet-scams-2022/

https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf

https://www.aarp.org/money/scams-fraud/info-2022/protecting-teen-targets.html

https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf

https://www.ic3.gov/Media/Y2022/PSA221025