Online Safety

Many people with 22q interact with others on the Internet. However, they may not be able to detect potential problems in their online interactions. Some have **lost money, been lured to meet in person to have sex, been bullied or abused, and gotten into other dangers**. This information sheet shows some of the known dangers online; however, scammers always find new ways to trick people. It is necessary to **be cautious and stay informed about potential dangers**.

How Scammers Get Your Money

1. A scammer sends an **email or text to get your banking info**

– The message may say there is a problem with your bank account or a package is waiting for you.

– The message may look like it comes from the bank, the postal service, the government, or a real company;

– The message asks you to click a link. The site asks for your banking PIN, credit card number, or e-transfer code, etc. **This info lets the scammer access your money**.

[QPS Delivery] Your parcel out for delivery with code UA-372-BR87 requires you to confirm your delivery preferences.
n8vs.info/h8v5ka23

Suspicious link. This is where the scammer collects your banking info.

(continued on the next page)

Signs That a Text Message or a Post Comes from a Scammer

- You did not expect to receive the message: text is not how your bank usually reaches out to you;
- The message **urges you to act quickly.** "Pay now", "The offer is only good until the end of the day", "Your (loved one) will be arrested if you don't pay now."
- The message says, "**Don't tell anyone**" or "Let's move the chat to a **private message**".
- The message asks for **cash, cryptocurrency, banking info, credit card info, gift cards** etc.
- **The images seem to be made by artificial intelligence (AI).** For example, the number of fingers are incorrect, the reflections or shadows do not make sense.

Signs That an Email Comes from a Scammer

From: authenticationmail@trust.ameribank7.com
To: johnsmith@email.com
Subject: **A new login to your bank account**

The "From" email address domain is not from the real bank

Bank of America

Wrong logo and font

Dear account holder,

The message is not addressed specifically to you

There has been a recent login to your bank account from a new divice:

Spelling error

IP address: 192.168.0.1

Location: Miami, Florida

4 new transactions have been made with this account since your last login.

If this was not you, please reset your password immediately with this link:

https://trust.ameribank7.com/reset-password

Thank you,

Bank America

Inconsistent bank name

Suspicious link. This is where the scammer collects your banking info.

The message **makes you feel like you need to act now.** Examples include: "Pay now", "The offer is only good until the end of the day".

To learn more, visit the US Federal Trade Commission's Consumer Advice on **How To Recognize and Avoid Phishing Scams**

Graphics from Magnific.com – Teen boys using computers and Wikipedia – Phishing.

Online Safety (continued)

How Scammers Get Your Money (continued)

2. Build **a close relationship** with you
   - A scammer **tries to become your friend or romantic partner** on social media and gains your trust. Important: Scammers may not tell the truth about who they are. For example, an older man may claim to be a young woman.
   - Once the scammer gains your trust (and affection), they claim to have a financial need: e.g. a big medical bill, a relative in debt, an investment that needs funds etc. They **ask you to send money, cryptocurrency, or gift cards**.
3. **Pretends to be your relative** who needs money
   - A scammer sends a message and pretends to be a relative who got into an accident or is in trouble with the law etc. They **pressure you to send money very urgently**.
4. Makes a **fake video of famous person** asking you to invest/help
   - A scammer uses artificial intelligence (AI) to make a **deep fake video** of someone well-known inviting you to **invest in a worthy cause, donate money for disaster relief**, etc.
5. A scammer **promises you will win big or get a good deal**
   - A scammer tries to convince you to take advantage of a good deal by making a transaction. E.g. You won a cruise and need to pay to secure your spot; something is on sale but you **must pay now**.

Don't Give Away Your Info on Social Media!

What you post on social media may give scammers the answers to your banking security questions, e.g. your birthday from your photos or your mother's maiden name.

Rage Bait: Using Your Time to Get Them Money

Some scammers post comments or videos that upset people on purpose. Readers then post angry comments and debate with the content creator. The responses increases the engagement and ad revenue for the content creator but **wastes the readers' time and takes an emotional toll on them**.

Don't Believe the Sweet Talk!

Some **scammers meet their victims offline and sexually assault them**. For info on staying safe during outings, see p.2 of our sheet on Social Life and Personal Safety.

Parents should keep an eye out for unexplained mood, social withdrawal, and decreased appetite. While these changes may be "typical" for teens, they may also be signs of bullying and abusive relationships.

Online Safety Tips

- **Check before you click. DON'T RUSH!** Does the link lead to a proper website or one that steals info?
- **Don't** open attachments from unknown senders;
- **Do** use a screen name online, not your real name;
- **Never share your passwords, credit card numbers, address, phone number, school name, etc. online**;
- Set up parental controls, spam filters, security software, etc.;
- Update your software and your phone for better security; but **only update from official sources such as your phone's settings app**;
- Terms and conditions may be long and hard to read. To find out what social media (and other sites) actually do with your data, check out Terms of Service; Didn't Read.

References / Resources

- Terms of Service; Didn't Read – International (volunteer based)
- Online safety for young people with intellectual disability – eSafety Commissioner, Australia
- How to Recognize and Avoid Phishing Scams – Consumer Advice, Federal Trade Commission, USA
- Common types of fraud and how to protect yourself | How to avoid social media fraud – National Bank, Canada
- Internet Safety Issues for Adolescents and Adults with Intellectual Disabilities – 2016
- Updated clinical practice recommendations for managing [children | adults] with 22q11.2 deletion syndrome – 2023

International 22q11.2 Foundation

The mission of the International 22q11.2 Foundation is to improve the quality of life for individuals affected by chromosome 22q11.2 differences through family and professional partnerships.

Joanne C. Y. Loo, PhD; Natalie Blagowidow, MD; 08/2026