ONLINE SAFETY FOR TEENS AND ADULTS WITH ASD

SARRC

Southwest
Autism
Research &
Resource
Center

ABOUT THIS MANUAL

ONLINE SAFETY STARTS AT HOME

Online life is rife with danger, and it can be difficult for families and professionals working with teens and adults with autism (ASD) to monitor the risks these individuals are taking in the virtual world. Getting knowledgeable about internet safety and arming them against the obvious dangers can build a foundation for the support they will need to safely navigate online.

This online safety manual was made possible by the generous support of NEXT for Autism. With funds from a two-year grant, the Southwest Autism Research & Resource Center (SARRC) was able to create an approachable curriculum that can be used to teach individuals with ASD the important skills needed to safely interact online.

Over the course of this grant, we have learned more about the risks associated with online activity, and we know individuals with ASD may be especially vulnerable to those risks. One of the core features of ASD is difficulty with social communication. When you add in the social nuances in an online environment, these social challenges can be magnified, essentially making social interactions even more difficult to interpret.

At SARRC, we have seen firsthand situations where the complexities of the social world online are misunderstood, and individuals have shared sensitive information putting themselves at risk for exploitation. Education, employment and even social opportunities all utilize and, in many cases, require an online presence, so it's imperative that those with autism better understand what types of activities to avoid and how to be safe when online.

Our hope is that this manual will support individuals and their families in safely navigating within an online community.

94%

94% of teens who use a mobile device go online at home daily.

~ Pew Research Center

SARRC Southwest Autism Research & Resource Center

STRATEGIES AND GENERAL GUIDANCE FOR TEACHING

As you begin to use this curriculum, there are a few important things to consider. When teaching these skills, it is important to remember to individualize the programs for each learner and be sure to take the content and adapt it in a meaningful way. The curriculum is intended to provide an overview of the important topics to cover with possible ways to teach the lessons as you work with teens and adults with ASD.

We advise that as you begin to teach these skills, do not start online. Instead, we recommend that teaching begins offline through the use of interactive PowerPoints, live role plays and scenario-based, decision-making models to contrive the situations we describe. This allows the individual to make errors in a safe environment. Once the individual is fluent in safe online behaviors, move teaching online using some of the monitoring resources we provide in section three for parents and caregivers.

This manual is divided into three sections with resources and a sample test to track online safety knowledge prior to beginning the curriculum and after completion.

CONTENTS

SECTION ONE:

SECTION TWO:

SECTION THREE:

SECTION ONE:

ONLINE SAFETY TOPICS FOR TEENS WITH ASD

■ COMPUTER SAFETY TIPS ■

One of the most common online safety mistakes teens can make is opening dangerous links or visiting unsecure websites when online. These actions can lead to unintentionally downloading a virus or providing personal information within an unsecure site, leading to identity theft, money loss or more. This mistake can often happen when an individual does not pay attention to the important features of a link or website address. Begin with the basics and teach about spam, spoofing, phishing and searching the web.

HOW TO TEACH:

Discrimination training
Multiple exemplar training
Behavioral skills training
Chaining

CONTENT TO COVER:

VOCABULARY

Spam: Bulk electronic communication often sent through email and often unsolicited.

Spoofing: Changing an email, website, link or other electronic information slightly to trick someone into trusting the source.

Phishing: When a spoofing technique is used to lure someone into providing private information. Criminals then use this information in dangerous ways.

Ghosting: When a person breaks up with someone or terminates a friendship by cutting off all contact with that person.

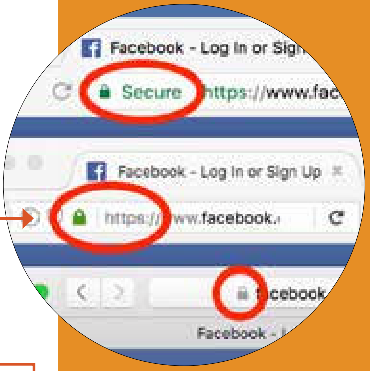
THINGS TO NEVER DO

- Give out email address or post email in a public space
- Open links from an email that you don't recognize
- Open emails or links that are labeled "junk" or "spam"
- Click on pop-ups that offer prizes
  - Search the internet using certain terms or phrases:
  - Illegal Drugs – making, buying, selling or how to take
  - Weapons & Bombs – Making, buying, selling
  - Murder/Assassination – How to
  - Girls/boys with any other word related to a preferred topic of interest
- File share or send saved photos or documents to someone online that you do not know

THINGS TO ALWAYS DO

- Set up filters in your email settings to identify junk and spam
- If you get an email that looks unusual, report this as spam or junk
- Have security software installed on your personal computers

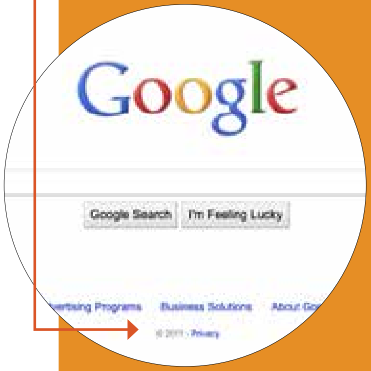
- Identify important features of websites
- When navigating online, the most important tool to use is your common sense. Does a website look strange to you? If it looks unsafe, don't take the risk.
- Look for signs of legitimacy. If doubtful, contact them by phone or email to obtain website information. Legitimate websites should have contact information listed.
- Remember to use secure, password-protected Wi-Fi whenever possible and to sign out of any websites you have accessed with passwords.



HOW TO TELL IF A WEBSITE IS SECURE:

CHECK FOR THE LOCK ICON

Secure websites will include the lock icon in the URL, while spoofed sites will not have one or may show a lock with a red X.



CHECK FOR A PRIVACY POLICY LINK ON THE WEBSITE

Nearly all websites will have a privacy policy listed on their website. This will explain what policies are in place to protect the people on the site. If a website does not have this, you should leave the site and be sure to not provide or type any personal information into the website.

■ ONLINE RELATIONSHIPS ■

Social relationships can be difficult to navigate and prove to be even further complex when they occur online. Understanding the difference between online friendships and real-life friendships; social media rules; what, when and how to share personal information online; and how to identify and respond to cyberbullying and cyberstalking are all important skills to teach.

HOW TO TEACH:

Discrimination training
Multiple exemplar training
Behavioral skills training
Chaining
DRO procedures
Token economy

CONTENT TO COVER:

DIFFERENCE BETWEEN ONLINE FRIENDS AND REAL-LIFE FRIENDS

Real-life friends are individuals that you have met in person, someone with whom you have shared experiences, someone that you trust and someone with whom you enjoy spending time. Online friends could be real-life friends that you also engage with online or they could be people that you have met few times or only met through online engagement. Online-only friends are those people you have never met or perhaps met just a few times. Online-only friends will often have shared interests with you or you may have shared friends. Online-only friends may be people you trust but often do not have the same level of trust as a real-life friend. Often when an online-only friend becomes a more trusted person in your life, you work to develop a real-life friendship.

When to send or accept a “FRIEND REQUEST”

If the person is someone you have met at least once in person

If the person is someone you like to interact with

If the person is someone you know through a shared friend

Social media DO’s AND DON’Ts:

Always set privacy settings to ensure only you can see your personal information. This includes information about where you live, your email, your phone number or your birthday

Choose sensible, strong, hard-to-guess passwords; do not use the same password for multiple sites

Always review and set privacy settings to limit who can see your posts; consider allowing close friends only

Always
use a secure browser

Never
post something that would be considered private or confidential, this includes talking about sex or posting inappropriate pictures or language

Be thoughtful
about how much you post each day and limit the number of posts you have on any given topic or interest

Never
tag another person without checking to see if they are comfortable

Do not accept a friend request from someone that you are already friends with -- this is often a scam and your friend's account was likely hacked

Be selective
when adding friends

Always ignore, block or report someone if they send you things that make you feel uncomfortable

Never repeatedly send a message to someone. If they do not respond right away, wait at least one day to send again. If they do not respond after three messages, do not send anything else unless they reach out to you.

■ SHARING PERSONAL INFORMATION ■

Personal information is private or confidential information about yourself. This type of information might include: social security number, your address, your phone number, your financial situation or bank information, your health status, or other important information that you would not want shared with strangers.

Sharing personal information online is dangerous because hackers and scammers may use your information to commit fraud or engage in other dishonest activities.

EXAMPLES OF APPROPRIATE TIMES TO SHARE PERSONAL INFORMATION

EMAIL

- Someone you just met and want to reach out to or talk to again
- Applications (volunteer, jobs, memberships)
- Online accounts on secure websites

SOCIAL MEDIA PROFILE

- Someone you met and want to interact with again
- Friends or family you want to keep in touch with

PHONE NUMBER

- Someone you already know
- Someone you have met a few times and want to get to know better
- Applications, if required
- Law enforcement

ADDRESS

- People you know very well and trust
- Transportation company (Uber, Lyft)
- Applications, if required
- Law enforcement

DEBIT CARD INFO

- Online purchases on secure websites
- NEVER give anyone your PIN number
- NEVER send through text, email, messaging
- NEVER take a picture of your card and send it to someone

BANK INFORMATION

- When you are talking to a teller at the bank or calling the official bank number

69%

69% of teens regularly receive personal messages online from strangers.

~ Cox Communications

- Employers; only if you want to set up direct deposit
- Setting up AutoPay on a secure site
- Parent/guardian if necessary

***NEVER give out personal information by text, email, dating sites, social media**

■ CYBERBULLYING AND CYBERSTALKING ■

Cyberbullying and cyberstalking is bullying or harassment that happens online. Cyberstalking is when the bullying behavior online happens repeatedly. This behavior can be directed at a person or a group of people. Cyberbullying and stalking can be considered a crime.

HOW TO KNOW IF IT IS HAPPENING TO YOU:

- Cyberbullying is when someone intentionally harasses, mistreats or makes fun of you online or while using cell phones or other electronic devices.
- Cyberstalking is when someone will not stop reaching out to you on social media or through other technology, even after you have asked them to stop.

WHAT TO DO IF YOU ARE BEING CYBERBULLIED:

- If the person has been a friend, ask them to stop.
- Tell someone you trust if you are feeling bullied online. Show them the messages.
- Block the person if they continue to bully.
- If the bullying continues, report to local authorities.

37%

37% of middle and high school students have reported being cyberbullied at some point in their life.

~ Cyberbullying Research Center

■ SELF-MONITORING ■

Research has found that significant amount of time spent online leads to an increase in the probability of being at risk for exploitation. As such, teaching teens how to monitor their time online is as important as how to interact safely online. Consider multiple target behaviors for self-monitoring programs, including appropriate, safe web-searching; time spent online; sharing safe information, etc.

HOW TO TEACH:

DRO procedures

Token economy

CONTENT TO COVER:

- Create self-monitoring goals and definitions together
- Carefully consider what a reasonable time-based interval will be for each monitoring period (Ex: 1 hour intervals would be too long for reporting on safe online behavior, but might be right for time spent online.)
- Have the teen collect data on their own behavior and have a second person also collect data and then check for agreement.
- Be sure to set goals and reinforcement on accuracy first, and then both accuracy and goal attainment.
- Start with achievable goals in terms of time online and make sure to create long-term goals for maintaining safe and appropriate amount of time online.

EXAMPLE OF COMPUTER USE DATA SHEET:

When the timer goes off, circle the + if you followed the safe searching tips, circle the - if you did not follow the safe searching tips.

INTERVAL	+ or -
1	+ / -
2	+ / -
3	+ / -
4	+ / -
5	+ / -
6	+ / -
7	+ / -

SECTION TWO:

ONLINE SAFETY TOPICS FOR ADULTS WITH ASD

■ ONLINE DATING ■

Dating is a common life experience for most young adults. While dating can be challenging for anyone, the complex social interactions that occur within a dating interaction can be even more difficult for a person with ASD.

HOW TO TEACH:

Discrimination training
Multiple exemplar training
Behavioral skills training
Chaining

CONTENT TO COVER:

HOW TO IDENTIFY SAFE AND UNSAFE DATING WEBSITES:

- Learn about who visits the site/app and what they are looking for
- Some are targeted for people looking for casual relationships or sexual encounters (see example at right)

IMPORTANT CONSIDERATIONS WHEN PAYING FOR DATING SITES:

- Ensure secure site; understand how they protect your information by reviewing privacy policy
- Do not sign up for auto withdrawl from an account; ensure you are able to cancel at anytime
- Make sure you are getting something of value for the cost; review all the terms and conditions before signing up

MEETING SOMEONE IN PERSON AFTER CONNECTING ON A DATING SITE:

- Always have the first few meetings in a public place like a coffee shop; do not share personal information like home address
- Consider having a close friend join you at the first meeting
- Tell people you trust where you will be and who you will be with and check in by text throughout the date

eharmony

eHarmony.com: A popular dating website and app with users looking to find long-term love in a relationship.

eHarmony.com
vs.
Tinder

tinder

Tinder: A dating app where users are asked to “Swipe Right®” if they are attracted to a person. The app has a reputation for users looking for “hookups” or casual sexual encounters.

WHAT IS CATFISHING?

When someone disguises themselves as someone else online to seduce and often take advantage of another person.

HOW TO IDENTIFY WHEN IT HAPPENS:

- Search photos someone sends you to see if they are stock photos from online images or if they come up as another person's name
- Be suspicious of anyone who asks you for favors or to borrow money or other things early in meeting them
- Someone is likely catfishing if they start to threaten to report you to police if you don't do what they ask

WHAT TO DO:

- Never send private or sexually explicit photos to someone online
- Seek help and advice from a trusted friend
- Block them from phone, social media, email
- Alert local officials

MONEY EXTORTION

Money extortion online can happen when someone misinterprets an online relationship and can lead to serious consequences, including federal criminal charges. It is important that individuals learn how to protect their financial information and can discriminate when an online money scam might be occurring and what steps to take.

HOW TO TEACH:

Discrimination training
Multiple exemplar training
Behavioral skills training

CONTENT TO COVER:

What is it? Money extortion is financial exploitation and is a form of fraud. Financial exploitation is one of the fastest-growing forms of abuse targeting adults with disabilities. Financial exploitation can happen by a known friend or family member or can occur through a scam or blackmail. Online financial exploitation often occurs after a time of grooming where the person is approached and a relationship is developed, which then leads to an ask of the individual.

TYPES OF EXPLOITATION:

Scams: Emails or texts that suggest someone has won something. The email or link asks someone to send their financial information to receive the prize.

Money Laundering: Asking someone to hold on to money or to accept money transfers and then withdraw the money and

50%

50% of adults with autism have been tricked or pressured into giving away money or their possessions.

~Aspect Research Centre for Autism Practice

give it to them, either through a 2nd money transfer or sending them money.

Unregulated loans: Loan from a person, often targeting someone that seems to need money quickly and does not understand how to borrow money in a safer way

Blackmail: Demands money or possessions after developing a relationship online and then threatens to share personal/private information.

HOW TO RESPOND TO REQUESTS:

- Never give out personal financial information
- Talk to a trusted friend or family member if someone is threatening
- Reach out to local law enforcement

PEOPLE WITH ASD MAY BE AT A HIGHER RISK FOR FINANCIAL EXPLOITATION BECAUSE THEY:

- Have difficulty navigating social cues and may miss cues that would suggest someone is trying to trick them into sharing information or allowing others to “borrow”
- May be overly trusting, they take people at their word and may not recognize when someone is lying or trying to deceive them
- Have difficulty telling others what is happening or what people are saying to them, especially if they have communication difficulties
- Lack advocacy skills
- May feel isolated or have limited social skills, this can lead to using the internet and social media to find friends, putting them at risk of online grooming

■ PORNOGRAPHY ■

Professionals and families have reported increases in porn addiction in their clients and loved ones in recent years. Aside from the obvious pitfalls of addiction, pornographic websites often have malware and other exploitive content. Additionally, some individuals with ASD connect socially with individuals younger than themselves and this can lead them down a dangerous path if they search for pornographic material that includes younger individuals/children. It is important that the skills needed to navigate safe and unsafe behaviors related to pornography are taught to reduce the possibility of engaging in illegal behavior.

HOW TO TEACH:

Discrimination training
Multiple exemplar training
Behavioral skills training

CONTENT TO COVER:

WHAT IS LEGAL OR ILLEGAL?

- Provide specific examples of what will get a person arrested and what will not.
- How and with whom to discuss pornography.

REALITY AND FANTASY:

- Porn is not usually an accurate reflection of relationships and sex
- Porn is often inaccurate and using it as a model can be harmful and could ruin relationships
- Some things happen in porn that never happen in real life

RULES TO FOLLOW:

- Only watch porn in private: Not in shared space at home and never in public spaces or at work
- Always have the door closed when watching porn
- Only use a personal computer, never a shared computer
- Only use appropriate search terms: man/woman, never boy/girl, teen
- Do not click on links in pop-ups
- Never download or save images or videos

■ CRIMINAL JUSTICE ■

Individuals with ASD may have a particularly hard time interacting with law enforcement. Additionally, people with disabilities make up a large portion of false confessions. Challenges with social communication and non-verbal communication can make interactions surrounding being arrested and questioned very difficult and may lead to inaccurate statements. It is important to teach individuals with ASD strategies for communicating with law enforcement and what to say or not say should they be questioned by law enforcement.

80%

Estimates suggest that 80% of pornogrphy is violent in nature.

~ Violence Against Women, Bridges et al., 2010

HOW TO TEACH:

Discrimination training

Behavioral skills training

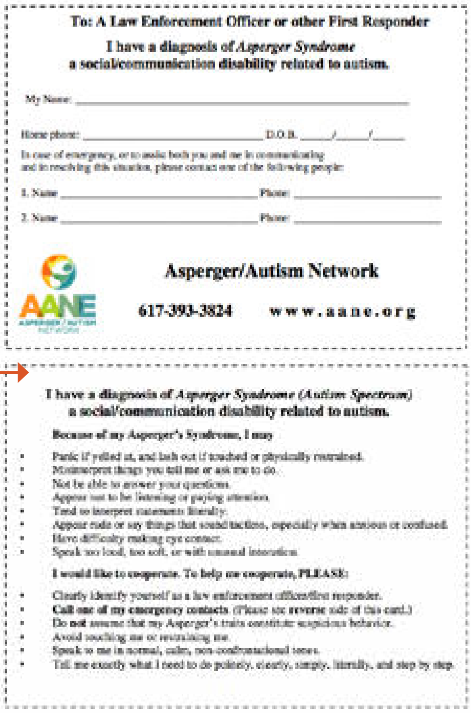
Role play

CONTENT TO COVER:

- Individual rights
  - You have the right to remain silent and not speak or answer questions
  - Anything you say can be used against you in a court of law
  - You have the right to an attorney and to have him or her present during any questioning
  - If you cannot afford a lawyer, one will be appointed to you free of charge
- You can waive your right to be silent before or during an interrogation, and if you do so, the questioning must be stopped
- If you want an attorney, no questioning can take place until he or she is present
- Importance of disclosure of ASD in these situations

LAWYERS AND ADVOCATES

- Must say, "I request a lawyer and an advocate"
- Do not talk until your lawyer is present
- Ask that any interviews be recorded
- Use of a wallet card that explains ASD, individual challenges and who can be called to help you if needed



To: A Law Enforcement Officer or other First Responder

I have a diagnosis of *Asperger Syndrome*
a social/communication disability related to autism.

My Name: ______________________________

Home phone: ____________________ D.O.B. ____/____/____

In case of emergency, or to assist both you and me in communicating
and in resolving this situation, please contact one of the following people:

1. Name ____________________ Phone: ____________________

2. Name ____________________ Phone: ____________________

Asperger/Autism Network

617-393-3824 www.aane.org

I have a diagnosis of *Asperger Syndrome (Autism Spectrum)*
a social/communication disability related to autism.

Because of my Asperger's Syndrome, I may

- Panic if yelled at, and lash out if touched or physically restrained.
- Misinterpret things you tell me or ask me to do.
- Not be able to answer your questions.
- Appear not to be listening or paying attention.
- Tend to interpret statements literally.
- Appear rude or say things that sound tactless, especially when anxious or confused.
- Have difficulty making eye contact.
- Speak too loud, too soft, or with unusual intonation.

I would like to cooperate. To help me cooperate, PLEASE:

- Clearly identify yourself as a law enforcement officer/first responder.
- **Call one of my emergency contacts.** (Please see **reverse** side of this card.)
- **Do not** assume that my Asperger's traits constitute suspicious behavior.
- Avoid touching me or restraining me.
- Speak to me in normal, calm, non-confrontational tones.
- Tell me exactly what I need to do politely, clearly, simply, literally, and step by step.

CONSEQUENCES OF CONVICTION

- Less inclusive educational opportunities
- Fewer social opportunities
- Limited or lost employment opportunities
- Jail or prison time
- Sex offender registry
- Limited housing opportunities

SECTION THREE:

INFORMATION FOR PARENTS/CAREGIVERS

While preventing use of the Internet is not possible or practical, limiting time spent online is a smart strategy for parents and caregivers because we know that the more time spent online, the greater the risk of exploitation.

■ TIPS FOR MANAGING ONLINE SAFETY AT HOME ■

- Keep your home computer in a shared location
- Review settings of all electronic devices and enable parental controls and restrictions as appropriate
- Download monitoring software (see next section)
- Establish time limits for electronics with Internet access
- Be familiar with your teen's favorite websites
- Communicate with your child about online bullying and his online activities
- Use technology together to learn what they are interested in and help with any challenges or online mistakes
- Enable safe searching settings on your browser or age-appropriate filters
- Teach your teen how to keep their social media settings "private"
- Limit computer and Internet time and encourage them to self-monitor their time online
- Monitor all credit cards for any unauthorized purchases
- Signs that a loved one may be at risk

■ SIGNS THAT A LOVED ONE MAY BE AT RISK ■

- The person spends significant amounts of time online, especially at night
- Pornography is found on the person's computer
- The person receives phone calls from adults unknown to you
- The person receives or makes calls to numbers the family doesn't recognize
- The person receives mail, gifts, packages from unknown people
- The person becomes withdrawn from daily life
- The person uses an account under a different name
- The person turns the monitor off quickly when others enter the room

■ PARENTAL MONITORING APPS ■

Numerous companies are constantly coming up with new technology that allows parents to monitor their children's online activities. Safewise came out with a list of "The Best Parental Control Apps of 2020," which can be found in the Resources section of this manual. Among the top picks for teens include these two apps:

BARK:

Developed to help alert parents to danger before something bad happens. Bark focuses on prevention, not just control. It looks out for signs of potential problems like self-harm, depression, cyberbullying, online predators, and extreme situations like school shootings.

- Monitors 24 different apps and social networks
- Scans emails, texts, photos and videos
- Delivers parental alerts along with recommendations from a child psychologist

QUSTODIO:

One of the most comprehensive parental monitoring apps available. There is a free basic version or paid tiers for access to extra features. One of the most popular Qustodio features is the panic button. Kids can access the panic button through the Qustodio app on their smartphone. When they hit the button, you get an instant panic alert — and thanks to location tracking, you can pinpoint exactly where your kid is when they call for help.

RESOURCES

LINKS TO ONLINE SOURCES

ONLINE SAFETY:

Safe Online Surfing for 3rd-8th Grades, Federal Bureau of Investigation
Consumer Information on Kids and Socializing Online, Federal Trade Commission
Consumer Information on Kids and Virtual Worlds, Federal Trade Commission

CYBER BULLYING:

Consumer Information on Cyber Bullying, Federal Trade Commission
Online Harassment and Cyberstalking, Privacy Rights Clearinghouse
12 Crucial Tips to Protect Yourself from Cyberstalking, ThoughtCo.

PHISHING:

How to Recognize and Avoid Phishing Scams, Federal Trade Commission

CATFISHING:

8 Tips to Protect Your Kids from "Catfishing" Online, Family Education
What Is Phishing, Spoofing, Ghosting and Catfishing? Bark Blog

PARENT TRAINING:

Keeping Up With Kids' Apps, Federal Trade Commission
Create a Technology Contract With Your Family, Bark Blog

SOCIAL NETWORKING AND PRIVACY:

Social Networking Privacy: How to Be Safe, Secure and Social,
Privacy Rights Clearinghouse
Online Privacy: Using the Internet Safely, Privacy Rights Clearinghouse
Facebook Smart Card
The Best Parental Control Apps of 2020, Safewise
Social Media, Gaming, Photo and Video Apps Explained, Protect Young Eyes

CRIMINAL JUSTICE:

ASDs and Involvement in the Criminal Justice System, Autism Awareness Centre Inc.
Asperger Syndrome in the Criminal Justice System, Asperger/Autism Network

MONEY EXTORTION:

Financial Exploitation, Disability Justice
Are autistic individuals vulnerable to financial exploitation?
Autism Spectrum Australia

PRE-TEST / POST-TEST FOR ONLINE SAFETY KNOWLEDGE

SCENARIOS:

A website pops up while you are checking your emails, it says you have won the lottery. They ask for your debit card information to send you the money you won.
What do you say/do?______________________________

You are filling out a job application and they ask for your name, email, phone number, and address.
What do you say/do? ______________________________

You meet someone at a store and they ask for your phone number
What do you say/do? ______________________________

A cousin you have grown up with but haven't seen for a few years asks for your address so they can come visit you.
What do you say/do? ______________________________

You get a message from someone who says they are a family member. They need you to send them money so they can fix their car. They ask you not to tell your parents because they are embarrassed.
What do you say/do? ______________________________

You met someone on a dating site and have been messaging for a few weeks. You set a date to meet up and grab lunch. They ask for your phone number to call you when they get there.

What do you say/do? ______________________________

You meet someone online and after a few minutes they ask for your address so they can come over.

What do you say/do? ______________________________

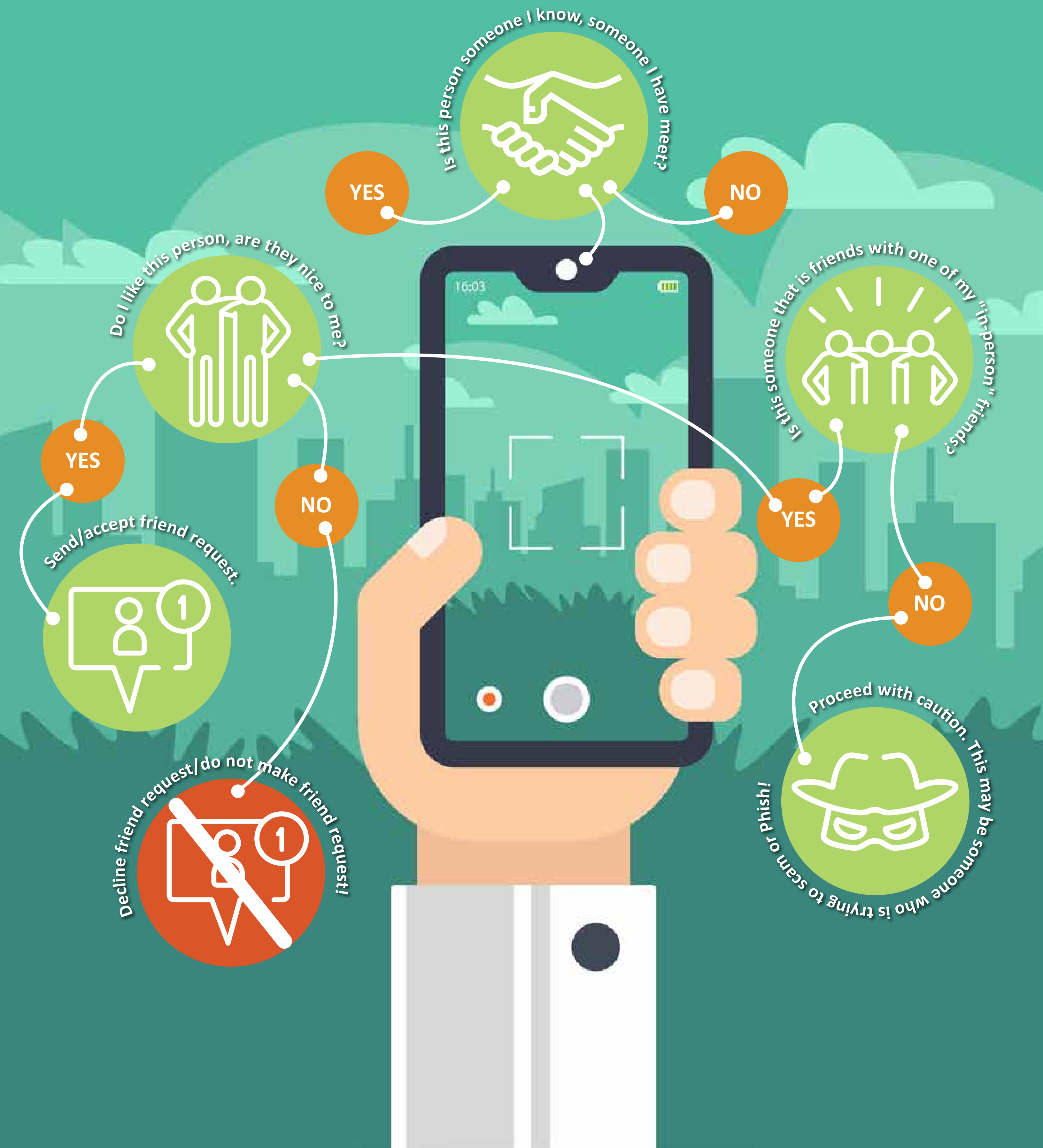
You see the same person at the library every week. You sometimes talk about cool books and movies you both enjoy. One day they ask for your phone number.

What do you say/do?

You receive a text from the bank asking you to update your PIN number. They ask you to enter your old PIN number followed by a new one.

What do you say/do?

WHEN TO "FRIEND" SOMEONE ON SOCIAL MEDIA



Is this person someone I know, someone I have meet?

YES

NO

Do I like this person, are they nice to me?

YES

NO

Send/accept friend request.

Decline friend request/do not make friend request!

Is this someone that is friends with one of my "in-person" friends?

YES

NO

Proceed with caution. This may be someone who is trying to scam or Phish!

SARRC

Southwest
Autism
Research &
Resource
Center

300 N. 18th Street
Phoenix, AZ 85006
Phone: 602.340.8717
Email: sarrc@autismcenter.org

Facebook.com/SouthwestAutism

Instagram: @SouthwestAutism

LinkedIn: linkedin.com/company/sarrc

Twitter: @SWAutismCenter

YouTube: @SouthwestAutism