milestone
CENTERS FOR PEOPLE WITH DEVELOPMENTAL & BEHAVIORAL HEALTH CHALLENGES

HCQU Northwest

Internet Safety Manual for Supporters:

Supporting Persons with Intellectual Disabilities & Autism to Stay Safe Online

Special Thanks to:

Alan McGill
Senior Supervisory Special Agent
Office of Public Engagement
Pennsylvania Office of the Attorney General

For his expertise and guidance in the development of the Internet Safety Modules

TABLE OF CONTENTS

INTRODUCTION

Milestone HCQU Northwest developed the Internet Safety Curriculum in response to frequent requests for supporting individuals with Intellectual Disabilities and Autism (IDA) to stay safe on the internet. People were putting themselves in financial, emotional, legal, and even physical danger because they clicked on the wrong link or believed in the honesty of the people they met online. Individuals overdrew their accounts, sent illegal contraband, or travelled somewhere from which they were unable to return, yet it was still difficult for supporters to convince some people that they were being scammed. Scammers are very convincing!

This manual is intended to provide you as a supporter information necessary to help individuals keep themselves safe. You may need to assist people when they have been scammed. You may need to help them recognize scams by making connections between what is being said and done to them and what tricky people say and do. Most importantly, the Internet Safety Curriculum is intended to educate people about potential scams before they occur. Education is the best method of prevention.

The **Internet Safety Curriculum** includes:

- **Training modules for individuals**. Each module takes 10-20 minutes to complete and may be watched as many times as desired. We encourage supporters to view and discuss with individuals when possible.
- **Self-guided tests**. Individuals will have the opportunity to connect what they have learned in the training module with real-world situations. They are provided choices for which incorrect responses lead to reteaching of the concept, then loop the person back to try again. Correct responses lead to a statement reinforcing the concepts and move the person forward through the test.
- **One-page handouts.** Individuals can download and print a handout that reviews the key information contained in the associated training module for easy reference.
- **A training manual for supporters.**

This manual includes the information provided in the training modules for individuals as well as supplemental information *(italicized)* related to those modules. Additional resources include information on where and how to report victimization related to various scams. You will also find tips for talking with people about Internet Safety. Lastly, we are including information about some other types of scams that are not explicitly covered in the modules. There are simply too many tactics used by scammers to cover them all without overwhelming learners.

PLEASE NOTE:
We attempt to be gender neutral as much as possible, frequently using the terms “they” and “them” (vs. he/him or she/her) in recognition of and respect for differences in sexual orientation, gender identity, and gender expression.

GENERAL INFORMATION

In order to combat the dangers of the internet, it is important to understand its allure. The internet provides:

- **Anonymity** — you can be whoever you want to be online. For people with I/DD in particular, it provides freedom from identification as a person with a disability.
- **Freedom from isolation** caused by lack of transportation and limited face-to-face interaction due to circumstances, disability, and/or limitations related to the pandemic.
- **The ability to explore and to connect** with others who share their interests.
- **Excitement —** an alternative to the hum-drum of everyday life.

SCAMMERS:

- Pretend to be someone they are not — a government official or law enforcement, a representative of a bank or credit card company, someone famous, a friend or family member.
- Prey on people who are sad or lonely. They develop online relationships with people, telling them they care about them and want to be their significant other.
- Design scams to create a strong emotional reaction, such as fear, love, pity, guilt, or excitement. They know that strong emotions make it more difficult to think things through.
- Tell you that you must act quickly, usually because you will miss out on an opportunity or there is some kind of problem or emergency that you need to address immediately. They want you to worry so you will hurry.
- Ask victims to keep secrets from people who look out for their best interests (friends, family).
- Request access to personal information.
- Do not always work alone. They often involve another person who they claim is a landlord, mechanic, etc., depending on the story they are telling.
- Contact victims by phone, text, and sometimes in person, in addition to email, social media, and other online contacts.
- May get "pushy" if you question them or try to stop contact.
- May use different types of scams together (ex. a romance scammer may pretend to be a successful investor leading a person to a fake investment).

Top Ten Countries Where Scams Originate

* Nigeria	* Indonesia
* India	* Venezuela
* China	* South Africa
* Brazil	* Phillipines
* Pakistan	* Romania

https://www.analyticsinsight.net/top-10-scamming-countries-in-the-world-in-2021

KEY CONCEPTS TO REVIEW WITH LEARNERS

NEVER give anyone your personal information, no matter how much you care about them or how important they say it is.

PERSONAL INFORMATION

- Full name
- Address
- Social Security number
- Cell phone number
- Usernames & passwords
- Bank account numbers
- Credit/debit card numbers

Scammers request money via untraceable means (NOTE: digital/cryptocurrency is growing in popularity amongst scammers).

UNTRACEABLE FORMS OF PAYMENT

- Prepaid cards
- Gift cards
- Digital wallets/cryptocurrency
- Money transfers

If you have any concerns or recognize any warning signs that someone might be a Tricky Person, STOP contact with that person right away.

It is ok to stop online contact with anyone, at any time, for any reason. This is not being rude — this is being safe!

There is no way to permanently delete something once it is online, so NEVER send anything (especially pictures and videos) that you wouldn't want anyone and everyone to see.

GENERAL TIPS FOR PROVIDING SUPPORT

If someone comes to you for help, this means that they trust you! Remember to always honor that trust.

Be prepared to help the person go through the processes necessary to address the concern. They may need to block the person from their account/s and/or report to law enforcement, government agencies, banks, or credit card companies. It can get very complicated, very quickly.

If someone has been scammed:

- Reassure them they did nothing wrong. The tricky person is the bad guy (or gal)!
- Discourage the person from deleting contacts with the scammer. They may want to, but law enforcement may need that information.

The Modules

OVERVIEW OF THE MODULES

The training modules in the Internet Safety Curriculum are designed to stand alone while still maintaining certain consistencies between modules. For example, the individual is represented by an emoji and the scammer is represented by a black hooded figure. To reinforce the reality that scammers try to trick you, we consistently refer to them as "tricky people." We use scenarios and examples to reinforce key concepts. Visuals and animations are used to enhance the learning experience.

The following modules are available:

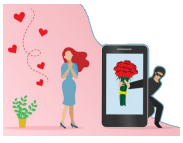
Tricky People – an overview of tactics used by scammers that introduces the learner to the basic concepts used throughout the modules.

Fear Tactics – scammers want to create strong emotions so victims will act quickly, without thinking it through. They often do this by making victims feel afraid for their own well-being or that of someone they care about.

Identity Theft – once a scammer has a victim's personal information, they can assume their identity online to steal from the victim in various ways.

Phishing – ("fishing") scammers can use very sophisticated means of tricking you into giving them your personal information, so knowing what to look for is key.

Romance Scams – another strong emotion used by scammers is love – unlike some online scams, romance scammers may take weeks, months, or even years to build trust with their victims. Their intent is to convince victims that they love them before they ultimately ask for money or personal information.



While there is no prescribed order, we recommend beginning with Tricky People, since it provides an overall picture of the basic tricks scammers use and introduces the learner to some of the basic terminology.

Tricky People…

Pretend to be your friend – they say & do things that a real friend would do, like give you compliments.

Pretend to be someone else using fake pictures of themselves and made-up stories about their lives.

May pretend to be someone famous, like an athlete, actor, or singer.

May pretend to be someone from a real place, like your bank, the IRS, the Social Security office, etc. and tell you they want to help you get or stay out of trouble.

Look for people who are having a tough time – people who are sad or lonely.

Pretend to care about your problems. They ask you questions about your life. They want you to think they are really interested in you.

May offer you gifts for no reason. They spend a little bit of money on you in order to get more from you once you trust them.

They often seem to like everything that you like.

Sometimes wait a long time to build your trust in them before they ask you for anything (money, personal information).

Might get "pushy" if you try to stop contact with them.

May threaten you to make you do something you don't want to do.

Tricky People know that the stronger a person's emotions are, the easier it is to trick them, so they might…

Try to make you feel bad for them by telling you they are in trouble.

Try to make you feel afraid that something bad will happen to you or someone you care about.

Try to make you feel excited that something too good to be true just happened to you.

Tell you they love you and want a romantic relationship with you.

It is important to remember

Don't give anyone your personal information.

Never post vacation plans online.

It is ok to stop online contact with anyone, at any time, for any reason. It is not being rude, it is being smart.

Fear Tactics

There are many scams that use fear to get people to give personal information. They typically revolve around fabricated issues that must be addressed quickly to fix a problem or avoid trouble (fees, fines, arrest) for the individual or someone important to them.

Tricky People say they are:

- From a government agency (Internal Revenue Service, Social Security, Medicare, etc.)
- From a financial institution (bank, credit card company)
- Law enforcement (constable, sheriff, state police, FBI, etc.)
- A service provider/utility company
- Computer virus protection
- Someone who cares about you
- A family member or friend

They might:

- Know some information about you when they call, like your name and address (easily obtained online), which makes them sound legitimate.
- Ask you to send payment to a third person who claims to be their landlord, lawyer, doctor's office, or whomever they claim to owe money.
- Fake the numbers on your caller ID to look legitimate. The same is true for emails – they might use logos and similar email domains that look like the real thing, if you don't look closely.

Reasons they give for contacting you:

- You owe money
- There is a warrant for your arrest
- There is a problem with your account (illegal activity, unauthorized access)
- Your computer has a virus
- They need your help (family/friend in trouble and need money right away)

What they ask for:

- Personal information; for example, they might ask you to confirm your identity by providing your Social Security number
- Payment (to bring your account current, avoid fees/fines/arrest, a fee for their services)
- Your help (money to avoid eviction, arrest, etc.)

Specific Scams Reviewed:

- IRS Scam - "*I'm from the IRS. You owe back taxes.*"
- Warrant Threat Scam - *"This is the police calling. There is a warrant for your arrest because you owe money."*
- Online Blackmail - *"I will make the naked picture you sent me public if you don't do what I say."*
- Fake Emergency Scam - *"This is your family member and I need money. Please help me!"*

FEAR TACTICS

"When you feel deeply afraid you'll do almost anything to get out of that state of being."

--Marguerite DeLeima, professor, University of Michigan

Some things to know:

- Government agencies do not call on the phone – they send a letter if they need to inform you of a problem.
- Computer companies will not call you unless you call them first.
- Law enforcement does not take payments over the phone – payments are arranged through the courts, not the police or FBI.
- Scammers will pretend to know something, trying to get you to "confirm" (your SS#, account number, etc.). They might say they are a friend/family member, but use a generic term like "best friend from school," "cousin," or "grandson" to get *you* to say a name.

If someone asks for money or personal information, hang up immediately!*

If the individual accidentally gave the scammer money or personal information, they may need to call the bank or credit card company to try to cancel payment (which may or may not be possible). *Additionally, they may be a victim of Identity Theft. What to do and who to contact will depend on what information was given. Please see the section on Identity Theft for more information on next steps.*

Report the (attempted) scam:

IRS Scam – 1-800-366-4484

Warrant Threat – local police

**If the individual is worried that they hung up on a legitimate caller, they may need help making contact to check on the call:*

1. *First, reassure the individual that hanging up was the right thing to do.*
2. *Remind them that if it was a friend or family member, that person would want them to be careful and stay safe. If it was law enforcement, a financial institution, etc., they also understand the need to protect oneself from scammers.*
3. *Then suggest they find independent contact information for that agency/office/person so they can call and check to see if the contact was legitimate. Just make sure they don't use the number given by the caller.*
4. *If they don't have the number for a family member, they may need to call someone close to the person who will know or can check to see if the person is truly in trouble (ex. call their aunt for their cousin's contact information).*

IDENTITY THEFT

Identity Theft

When Tricky People are able to get your personal information, they can use it to pretend to be you. Some common ways they use your information:

- Purchase items for themselves on your credit card.
- Sign up for credit cards in your name and have them sent to them instead of you.
- Transfer or withdraw money from your bank account.
- If they get your Social Security number, they can even file for and receive your tax refund!

General Tips for Protecting Your Identity:

Make sure to **always log out** of any site that might contain or provide access to your personal information, such as financial institutions, shopping sites, and social media.

Never give anyone your usernames, passwords, or PINs (Personal Identification Numbers) – this includes family, friends, and other supporters. Remember, no one should ever need your password for any reason.

If you need to write down usernames and passwords to remember them, keep them together in a secure location where no one else can access them, such as a locked box or drawer.

Do not use passwords related to information about you that anyone could find out, like the name of your pet or your birthdate.

At least once per year (or after any major data breach) schedule a session to address all of your online accounts:

Change passwords. Never use the same password twice, especially for critical accounts like bank and credit cards. Do a complete change, not just one letter/number.

Close out accounts you do not use. Start with the ones that email frequently that you never open.

Make sure to set a password for your voicemail, especially if you can access it directly from your phone. Tricky People can spoof your phone number to access your voicemail.

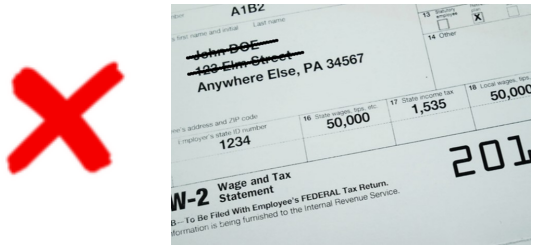
IDENTITY THEFT

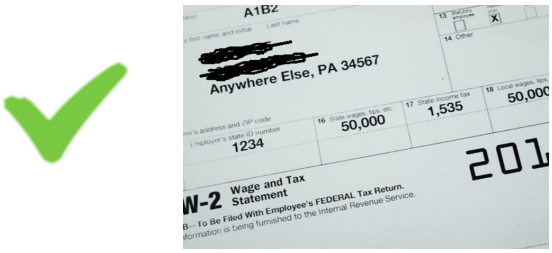
Protect Your Identity on Social Media:

- Don't accept friend requests from people you don't know. This is how a lot of Tricky People gain access to personal information, so the more "friends" you have, the more likely it is you will encounter a Tricky Person.
- If you get a friend request from someone who is already on your friends list, check with that person before accepting to make sure it is really from them.
- Limit what information others can see about you. You don't have to fill out all of the information on your profile – you choose what information about you other people can see!
- Even when you limit information on your profile, it's a good idea to keep your settings private so that only the people on your friends list can see your information.
- Different apps have different ways of setting privacy. You can usually find directions online. The following site contains instructions for some of the most popular social media apps: https://edu.gcfglobal.org/en/internetsafety/social-media-privacy-basics/1/
- Be careful what you post. Tricky People can get information from pictures (including images in the background) and information posted on social media. Where you work or go to school, where you worship, and organizations you belong to can all give people information about us.

Protect Your Identity at Home:

- Collect mail daily
- Don't throw out anything without first destroying any personal information it contains. Tricky People can go through your mail, find a credit card offer, change the address, and apply for a card in your name that will come to them for their own use. You will not even know this has happened until the credit card company reports you for non-payment. They may also find account numbers that they can use to access your money. Destroy the information by shredding the document, cutting it into very small pieces, or scribbling over the personal information, preferably with a Sharpie marker or pen – just make sure it can no longer be read.





Protect Your Identity in the Community:

- If you are entering usernames or passwords online while you are in the community or if you are entering your PIN in an ATM or at a store, be careful that no one is behind you and able to look over your shoulder to see what you are entering (this is called "shoulder surfing"). For example, try to sit with your back to a wall so no one can come behind you or angle your screen so that it cannot be seen by anyone around you. Block others' view of the PIN pad with your other hand or by standing between it and them.
- Only take what you will need and keep it secure in a wallet, purse, etc. that you keep with you at all times. You should never need your Social Security card while in the community, so keep it locked up at home at all times.

If credit/debit card numbers are lost, stolen, or given to a Tricky Person, it is important to report it to the financial institution/s as soon as possible. They will suspend the card so that no one – including you – can use it. They will issue a new card with new numbers. It could take up to two weeks to receive the new card, *so an alternative means of accessing money will need to be found in the meantime (for example, going to the bank and withdrawing cash). Also, remember to update the new numbers as soon as they arrive for any automatic payments that are set up using the old numbers. It is also a good idea to put a fraud alert on your credit report.*

There is no place to report a lost/stolen driver's license or identification. The same is true for a Social Security card/number. While both cards can be replaced, there is no means to stop someone from using the numbers. *If there is a possibility that someone has your social security number, you will need to keep a close watch on your credit report to make sure no one has taken credit using your name and Social Security number.*

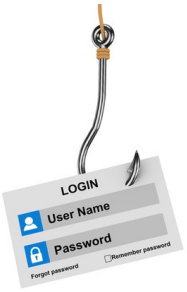
If you see charges you didn't make on your bank or credit card statements, *if a new line of credit that you didn't apply for shows up on your credit report,* or if you suspect for any reason that your identity has been stolen, report it immediately to your local police department or one of these websites:

www.usa.gov/identity-theft

www.identitytheft.gov

www.irs.gov

PHISHING



Tricky People use texts, emails, phone calls, or websites that seem real to scam you. Some of them are very good at "spoofing" – making an email or website look like it came from a real bank or (usually well-known) company, like Facebook, PayPal, or Amazon, using company logos and attempting to appear legitimate. Phishing is the most common internet crime in the U.S. *In 2020 in the U.S. $86 million was lost to scammers via fake texts alone.*

Sometimes Tricky People call on the phone, usually saying they are from a tech company calling to inform you of a problem with your computer. They offer to fix it for you once you pay them a fee by providing your bank/credit card number. Additionally, if you give them access to your computer, they can gather additional personal information that may be stored there.

Like most scams, phishing messages intend to create an emotional reaction in the recipient. They may make you feel excited, telling you have won something or that someone you don't even know has sent you money.

Most of the time, though, phishing messages tell you there is a problem that needs to be addressed quickly.

They might tell you:

- You've received an important document
- You need to renew or upgrade your account
- Your account is about to be suspended/closed
- Someone tried to log into your account
- Someone has your password
- Someone is trying to steal from you
- Your computer has a virus
- You owe money (via a fake invoice)

They want you to worry so you will hurry.

Different Types of Phishing:

Spear phishing -- targets a specific group or type of person*

Whaling -- going after a company's biggest "fish" – the CEO, CFO, etc.*

Smishing – uses text messages or a short message service (SMS). Ex. a text from your bank that your account has been compromised.

Vishing – attack via a voice call

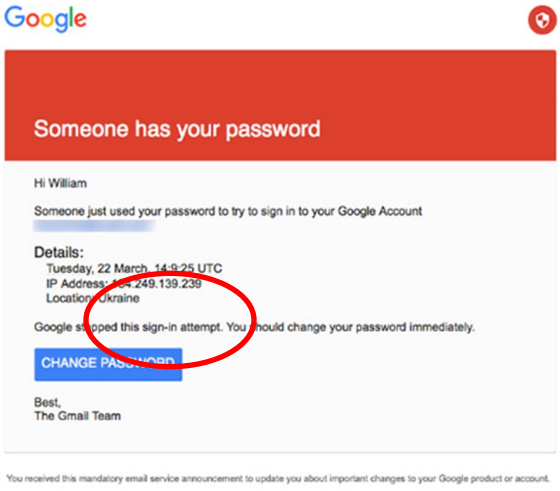
Email phishing – the most common type; what is covered in the module

**usually occurs in businesses/companies*

PHISHING

Phishing messages may ask you to reply with personal information. Most of the time, they provide a link that they encourage you to click to address the problem. These fake links will do one of two things:

- Take you to a fake website that usually appears real. This site will then ask for personal information like usernames and passwords or payment information via bank account or credit card numbers.
- OR the link will initiate a download of malware onto your computer, which will allow the scammer to access everything stored on your computer and to watch everything you do, like logging into your bank account or a shopping site.



(NOTE: ransomware may also be downloaded, allowing the Tricky Person to prevent you from accessing the contents of your computer until you pay a "ransom" for its return. Ransomware is more likely to occur within businesses rather than personal computers).

Messages from or links to .edu or .gov are usually safe, but, like all unsolicited contacts, make sure to look before you link. Search for the institution first and look for subtle differences. For example, an email from the National Credit Union Association would be a fake, although there is a National Credit Union Administration.

Messages may also include attachments that may be dangerous. The only safe file to click is a .txt.

Whenever you receive an unexpected message, ask yourself:

How does the message make me feel? Excited, like something too good to be true has happened to me? Worried that something bad will happen if I don't respond?

Then consider:

Does the message tell me I have to hurry to fix or prevent something bad?

Do I have to act fast to get the great deal or collect my winnings?

PHISHING

Look closely at the message for the following Red Flags:

- Misspelling/typos – real companies are very careful to send out messages that are correct *while scammers are sending out thousands of emails/texts so they are writing fast and don't care about mistakes.*
- Odd/unusual wording – *many phishing scams originate from foreign countries and their messages are often grammatically incorrect when they are translated into English.*
- The sender's email address does not match the company they say they are from.
- They are using a free email provider (gmail, yahoo, hotmail, etc.)
- Hover over the link (without clicking on it) to see the URL – where the link is actually going. **If it doesn't match, don't click!**
- *Mismatched emails and links might be obvious or very subtle. For example, "bankofamerica.com" vs. "bankofarnerica.com" or "microsoft/support" vs. "microsoftsupport."*
- *Phishing messages often appear too personal. They may address the recipient by first name when there's no connection (i.e., a bank they don't use or a package they didn't order).*
- *Real businesses don't send chain messages, so if the message is directed to multiple recipients, it is likely a phishing attempt.*
- *Legitimate companies do not use emojis, so their presence is a red flag.*
- *Scammers may use all capital letters to grab your attention – real companies don't typically do this.*
- *The time when the message was sent can be a clue as well. If it arrived to you in the middle of the night, it was likely sent during the day from a foreign country in a much different time zone.*

Hello!

As part of our security measures, we regularly screen activity in the Facebook system. We recently contacted you after noticing an issue on your account.

Our system detected unusual Copyrights activity linked to your Facebook account, please follow the link bellow to fill the Copyright Law form.

http://www.facebook.com/application_form

Note: If you don't fill the application your account will be permanently blocked.

Regards,

Facebook Copyrights Department

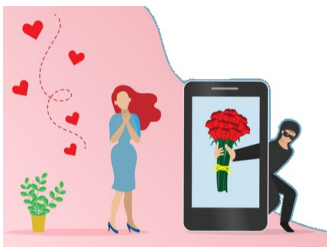
Additional Steps to Prevent Phishing:

- *Protect computers & mobile phones with security software set to update automatically*
- *Use multi-factor identification when available*
- *Back up computer & mobile phone data somewhere outside your home network*

Reporting Phishing attempts:

- *Forward phishing emails to: reportphishing@apwg.org (Anti-Phishing Working Group)*
- *Forward phishing texts to: SPAM (7726)*
- *Also report to the Federal Trade Condition (FTC) at: www.ReportFraud.ftc.gov*

ROMANCE SCAMS



Some tricky people pretend they want to have a romantic relationship with their victim. Unlike most scams, Romance Scams typically play out over a long period of time via multiple contacts while the scammer builds trust with the victim. Romance Scams are very common — it is estimated that one in every seven online dating profiles is fake!

Romance Scammers create an online persona that seems "to good to be true" to the victim:

- They have many, many things in common — they like they same music, activities, etc.
- They are usually very good-looking (because they are using fake pictures of themselves).
- They seem to care about the victim and their problems.
- They give their victim lots of compliments.
- They seem very romantic — they send love songs, give a special nickname, and frequently tell the victim how much they mean to them.
- They may send gifts, often for no reason other than their professed love for the victim. *This can be very confusing — victims may not understand why someone who was scamming them would spend money <u>on</u> them if their goal is to get money <u>from</u> them. They consider it an investment* — they spend a small amount of money on their victims now in order to get a much larger amount from them later.
- They tell their victim that they love them very early in the relationship. They say they want an exclusive relationship and may eventually ask the person to marry them.

> *"The criminals spend hours honing their skills, relying on well-rehearsed scripts that have been used repeatedly and successfully, and sometimes keep journals on their victims to better understand how to manipulate and exploit them."*
>
> *--FBI Press Release 2/10/21*

ROMANCE SCAMS

Romance Scammers always say they live (conveniently) far away from the victim. They might say they are from another country or that they are an American living/ working there. It is very common for a Romance Scammer to say they are in the military and are or about to be deployed overseas. Another common story they tell is that they are isolated out on an oil rig in the ocean (again, somewhere the victim cannot easily visit).

Because they don't want to risk being found out by the people who care about the victim, they often ask to meet on private chat sites and might ask the victim to keep their relationship secret from their friends and family. They say they want it to be their "special secret." They know that people who are not emotionally connected to them are more likely to recognize their scam.

They try to make their victim feel bad for them by saying they have no family or are out of contact with them, so they have no one else to ask for help when they need it.

They say they "can't wait" to meet in person. They might even make specific plans, but every time, something happens to prevent them from meeting — their car broke down, they are being deployed, or they don't have money for a ticket (hoping the victim will offer to pay or even asking them directly for money).

Eventually, they claim they have an emergency:

- They were in a car accident and can't afford repairs
- They were robbed
- They are about to be evicted
- They were hurt and have medical bills
- They need to sell their vehicle before they are deployed
- They need someone to claim their death benefits for insurance forms

While these are some of the more common "emergencies," tricky people can be very creative when making up reasons they need something from their victim. It might relate to something the victim is likely to know little about, making them less likely to see through the lies. For example, the scammer might say they need money for docking fees so they can get their ship out of port to make money with it. Whatever the reason, their goal is to make the victim to feel bad for them and to convey that it must be addressed quickly, before the victim has time to think it through.

Certain aspects of their story often won't add up and may even be contradictory. For example, they may say they were unable to do something, then later state that they did it. They may use terminology that doesn't make sense, such as a military person calling fellow soldiers "colleagues."

Their stories are often so heart-breaking and they sound so desperate that victims offer to help before the scammers even have to ask. When they ask for money, they will usually promise to pay it back as soon as they can. They ask the victim to send money (via untraceable means), either to them or to someone on their behalf (a "landlord," "mechanic," etc.). Requests for personal information typically center around the need to fill out paperwork to include the victim in their life somehow.

Unfortunately, by the time loved ones find out, the victim is often so convinced of the person's love that it is difficult for them to see the truth. When you are supporting someone caught up in Romance Scam, it is important to remember that they may react poorly when you try to tell them that the love of their life is a fake.

Rather than confronting the person with what is obvious to you, begin by asking questions.

You might suggest that you review the Romance Scams handout or even watch the training again. Gently ask whether the person in question has ever used the tactics listed.

Reassure the individual that they deserve to be loved for real, not by someone who would trick them and steal from them, so you just want to help them make sure the relationship is legitimate.

It may also be helpful for them to know they are not alone – many, many people each year get caught up in Romance Scams. The person should not be embarrassed because they did nothing wrong. The Tricky Person is the bad guy (or gal)!

Data from the Federal Trade Commission for 2021

* The primary origins of Romance Scams were Facebook (23%) and Instagram (13%)
* Top methods of payment (by $ amount) [by % of victims]:
  - Cryptocurrency ($139 million) [18%]
  - Bank transfer/payment ($121 million) [13%]
  - Wire transfer ($93 million) [12%]
  - Gift or reloadable card ($36 million) [28%]
  - Payment app/service [14%]

One of the quickest ways to check out a new contact is a reverse image search:

1. Go to images.google.com
2. Click on the camera icon
3. Cut and paste (or click and drag) the person's photo or it's URL into the search bar.

4. Look at the search results for terms like "stock photo" or for online photo source like shutter-stock or istock.

5. Look for information about when & where the photo was taken. Does it match what the person said?

Remember: not all fakes will show up in a reverse image search — a person can use their own picture and name and still be a scammer.

Other Types of Scams

SOME OTHER COMMON TYPES OF SCAMS (NOT INCLUDED IN MODULES)

Charity Scams

Most common around the holidays and after disasters, scammers trick people into believing they are donating money to a good cause.

They may pose as a known charity or make up their own.

Scammers frequently use crowdfunding apps, such as gofundme, but can also create fake emails, websites, and social media posts. Some charity scams involve direct contact with the victim, by phone or in person.

DO:

- Pay by check
- Write the check to the organization, not an individual
- Make sure you get a detailed receipt
- Look for .org (legitimate organizations do not use .com)

DON'T:

- Pay with untraceable forms of payment
- "Update" your information based on an unsolicited call from a charity to which you have donated in the past
- Cave in to pressure or guilt – not wanting to get scammed is not the same as not wanting to help

What to look/ask for:

- The organization's EIN (tax ID) number
- Search the name of the charity followed by "scam"
- Check a charity watchdog site:
  - Charity Navigator (charitynavigator.org)
  - Charity Watch (charitywatch.org)
  - Better Business Bureau (bbb.org)
- Check government sites
  - Charities.pa.gov/ (look at financial info of org)
  - Apps.irs.gov/app/eos (registered w/IRS as tax exempt?)

SOME OTHER COMMON TYPES OF SCAMS (NOT INCLUDED IN MODULES)

Holiday/Online Shopping Scam

Credit card fraud, non-delivery of items or counterfeit items ordered from a fraudulent company.

- Know who you are buying from. Research any unknown company. Check reviews.
- Check the URL. Is it a legitimate and secure site? Any site you purchase from should have "https" in the web address. If not, don't enter your information.
- Always remember: if it sounds too good to be true, it probably is.

When making payments to online sources

- Never wire money to a seller.
- Do not pay with pre-paid cards.
- Do use a credit card and check your statement regularly. If you notice anything suspicious, contact the company to dispute it.
- Always get a tracking number to ensure shipment and follow the delivery progress.

Malicious Quick Response (QR) Codes

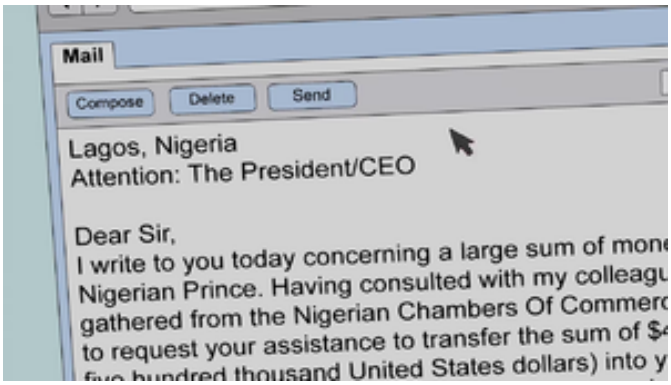
Cyber criminals tamper with the physical or digital square barcode meant to be scanned with a smartphone camera to provide quick access to a website, application, or to make a payment.

- After you scan the QR Code, check the URL. Does it go to the intended site? Does it look authentic? Beware of spoofing – look closely!
- Check physical codes for signs of tampering; for example, a sticker with a new code placed over the original on the product.
- Use your phone's app store to download any apps (vs. using a QR Code).
- Do not use any QR Codes sent from companies asking for money. Use contact information you already have, or from an online search for the company's contact info to check with the company.
- Don't make payments to a website accessed through a QR Code.
- Do not download a QR Scanner app – most phones have them built in.

Report any QR Code scams to ic3 (www.ic3.gov) and your local FBI field office.

SOME OTHER COMMON TYPES OF SCAMS (NOT INCLUDED IN MODULES)

419 Fraud



This type of scam is also known as “the Nigerian letter scam,” (419 is the Nigerian criminal code violated by the scam) because it involves a letter or email to a potential victim that purports to come from a government official, a prince, or someone else of wealth and position. Their misfortune is an “opportunity” for the victim. They claim to be worth millions, and offer the victim a percentage for helping them get those millions out of their country or free up money which is currently inaccessible to them due to war, corruption, or political unrest.

They ask you to:

- Provide your bank account number so they can transfer the money to you for safekeeping (you will have to return it to them, of course, minus a hefty fee for your services).
- Provide blank letterhead stationery and personal information
- Money to cover taxes, bank or legal fees, bribes, etc. (which they promise to reimburse once they have freed their funds).

They provide a fax number or return email for you to complete their request/s.

While most victims only lose money, some victims have been lured to Nigeria and imprisoned.

NOTE: The basics of this scam have been around since the 19th century. It really took hold in Nigeria, which is how it came to be known as “the Nigerian scam,” but recent versions have come from all over the globe.

If you receive a letter or email that you suspect is a 419 Fraud:

- DO NOT REPLY in any way. Don’t let your curiosity get the best of you.
- Send the letter/message to:

  U.S. Secret Service — secretservice.gov/contact/field-offices

  Local FBI office — fbi.gov/contact-us/field-offices

  U.S. Postal Inspection Service (for letters) — https://www.uspis.gov/report

SOME OTHER COMMON TYPES OF SCAMS (NOT INCLUDED IN MODULES)

Money Mules

Individuals who (unknowingly or complicitly) transfer funds for another to launder money from illegal activities.

- They are promised easy money.
- They believe they are helping someone (as part of a romance scam or an employment scam)
- Their personal information is used without their knowledge after being collected from another scam; for example, non-payment/non-delivery, lottery, or investment scams.

Targeted populations:

- Elderly
- College-aged students
- Newly immigrated people

Potential Consequences:

- Identity theft
- Personal liability
- Lowered credit scores
- Inability to open future bank accounts
- Federal charges (mail fraud, wire fraud, bank fraud, money laundering, etc.)
- Prison (up to 30 years), fines (up to $1,000,000), even if the person participates unknowingly.

Prevention:

- Don't open a bank account or receive funds into your personal account as part of a job offer, for a romantic partner, or for anyone.
- Protect your personal information
- Search online for corroboration
- Check with your bank regarding anything suspicious

If you think you are being used as a Money Mule:

- STOP communications with and transfer of funds/valuables to the suspected criminal.
- Keep all communications, receipts, etc. to provide to law enforcement.
- Notify the payment provider (ex. your bank)
- Report to ic3 (www.ic3.gov) and your local FBI field office

For more information go to: www.fbi.gov/scams-and-safety/common-scams-and-crimes/money-mules

SOME OTHER COMMON TYPES OF SCAMS (NOT INCLUDED IN MODULES)

Apocalyptic Threat Scam

This is a fear tactic in which scammers tell victims:

- The pandemic/economy/environment/health care system/etc. is creating financial risk if they keep their money in traditional financial institutions.
- There are alternative, “safe” investments, such as “collectible” gold and silver coins, which they can broker.

They sell these to victims with up to a 300% mark-up of their actual value.

They charge victims undisclosed fees.

If someone is trying to sell an unknown investment:

- Contact your state’s securities regulator to see if the company offering the investment is registered, has gone through examinations, and is licensed.

TIPS FROM THE FEDERAL TRADE COMMISSION:

What to Do If You Paid a Scammer

Did you pay with a credit card or debit card?

Contact the company or bank that issued the credit card or debit card. Tell them it was a fraudulent charge. Ask them to reverse the transaction and give you your money back.

Did a scammer make an unauthorized transfer from your bank account?

Contact your bank and tell them it was an unauthorized debit or withdrawal. Ask them to reverse the transaction and give you your money back.

Did you pay with a gift card?

Contact the company that issued the gift card. Tell them it was used in a scam and ask if they can refund your money. Keep the gift card itself, and the gift card receipt.

Did you send a wire transfer through a company like Western Union or MoneyGram?

Contact the wire transfer company. Tell them it was a fraudulent transfer. Ask them to reverse the wire transfer and give you your money back.

MoneyGram at 1-800-MONEYGRAM (1-800-666-3947)
Western Union at 1-800-325-6000

Did you send a wire transfer through your bank?

Contact your bank and report the fraudulent transfer. Ask if they can reverse the wire transfer and give you your money back.

Did you send money through a money transfer app?

Report the fraudulent transaction to the company behind the money transfer app and ask if they can reverse the payment. If you linked the app to a credit card or debit card, report the fraud to your credit card company or bank. Ask if they can reverse the charge.

Did you pay with cryptocurrency?

Contact the company you used to send the money and tell them it was a fraudulent transaction. Ask to have the transaction reversed, if possible.

Did you send cash?

If you sent it by U.S. mail, contact the U.S. Postal Inspection Service at 877-876-2455 and ask them to intercept the package. To learn more about this process, visit USPS Package Intercept: The Basics.

If you used another delivery service, contact them as soon as possible.

https://www.consumer.ftc.gov/articles/what-do-if-you-were-scammed#:~:text=Contact%20your%20bank%20and%20report,they%20can%20reverse%20the%20payment.

TIPS FROM THE FEDERAL TRADE COMMISSION:

What to Do If You Gave a Scammer Personal Information

Did you give a scammer your Social Security number?

Go to IdentityTheft.gov to see what steps you should take, including how to monitor your credit.

Did you give a scammer your username and password?

Create a new, strong password. If you use the same password anywhere else, change it there, too.

If a Scammer Has Access to Your Computer or Phone

Does a scammer have remote access to your computer?

Update your computer's security software, run a scan, and delete anything it identifies as a problem. Then take other steps to protect your personal information.

Did a scammer take control of your cell phone number and account?

Contact your service provider to take back control of your phone number. Once you do, change your account password.

Also check your credit card, bank, and other financial accounts for unauthorized charges or changes. If you see any, report them to the company or institution. Then go to IdentityTheft.gov to see what steps you should take.

https://www.consumer.ftc.gov/articles/what-do-if-you-were-scammed#:~:text=Contact%20your%20bank%20and%20report,they%20can%20reverse%20the%20payment.

RESOURCES

https://www.aarp.org — topics range from basic online safety to specific topics like how to pay bills online safely. Many are presented as a series of tips, and are geared toward readers who may not be familiar with the ins and outs of online use. A general search for “internet safety” will yield several thousand results, so it is helpful to search for a specific topic (ex. “social media”)

https://www.consumer.ftc.gov/topics/online-security — a great resource for just about anything related to online security, including a Password Checklist, How to Protect Your Privacy on Apps, and information on several common online scams.

https://www.fbi.gov/scams-and-safety — includes information on common scams, internet-related information, resources for reporting fraud and crime, and links to additional government resources.

https://www.ic3.gov — while the FBI’s Crime Complaint Center is a reporting resource, it also contains information via news releases and national and state data related to internet crime via annual reports.

https://www.ReportFraud.ftc.gov — view fraud data for your state or metro area.

REPORTING

Federal Bureau of Investigation (FBI)

Internet Crime Complaint Center — https://www.ic3.gov

Allows reporting of internet crimes by the actual victim or a third party on the victim’s behalf

Field Offices locator — https://www.fbi.gov/contact-us/field-offices

Federal Trade Commission (FTC) — https://www.ReportFraud.ftc.gov

They do NOT resolve individual reports but they use information from reported scams to build cases against scammers, identify trends, and enhance public safety through education. They also compile and provide data on what is happening in local communities.