

The background consists of several large, overlapping triangles in various colors: red, orange, yellow, green, blue, and purple. The triangles are separated by thin white lines, creating a dynamic, geometric pattern.

SCAMMERS

are like
spiders...

The background of the slide is composed of several large, overlapping triangles in various colors: red, orange, yellow, green, blue, and purple. These triangles are arranged in a way that they point towards the center, creating a dynamic and modern aesthetic.

Watch out for them...

... or they'll trap you in
their web or on the
web.

The background of the slide is composed of several large, overlapping triangles in various colors: red, orange, yellow, green, blue, and purple. These triangles are arranged in a way that they point towards the center, creating a dynamic and colorful geometric pattern.

The best thing to do is...

STOP

The background of the slide is composed of several large, overlapping triangles in various colors: red, orange, yellow, green, blue, and purple. These triangles are arranged in a way that they point towards the center, creating a dynamic and colorful geometric pattern. The word "RELAX" is centered in the white space between these triangles.

RELAX

The background of the slide is composed of several large, overlapping triangles in various colors: red, orange, yellow, green, blue, and purple. These triangles are arranged in a way that they point towards the center, creating a dynamic and modern aesthetic. The word "THINK" is centered in the white space between these colorful shapes.

THINK

Some general advice

- Don't hurry when clicking on things on a website or in an email. Take your time and think it through.
- Read carefully and don't rush through just because you think you know what it says or is going to say.

Compose

Inbox 33

Starred

Snoozed

Sent

Drafts

More

Labels +

2021 Lenora

2022 Lenora

Friends 3

important save 4

Lenora Estate Plannin...

Jokes

Lenora 2019

Lenora emails 2016... 4

ambassadors

1 of 3

Your mailbox is full

GoDaddy mailbox@woodcroftwomensclub.org via bounce.secureserver.net

Fri, Sep 30, 5:34 AM

This message seems dangerous

Similar messages were used to steal people's personal information. Avoid clicking links, downloading attachments, or replying with personal information.

Move to spam

Looks safe

Your mailbox is full.

2 GB

1.9 GB

Your mailbox can no longer send or receive messages. Click here to make room in your mailbox.

Mailbox address:

Another “close to home” example...

10-21-22 Nextdoor notice:

Be careful, a woman claiming that she was getting donations for the YMCA came to my home, dressed like a YMCA employee and spoke to an elderly person in my house and asked to come inside saying that other neighbors had invited her in for dinner, she also asked for phone number, date of birth and other private information. The YMCA said that they do not door to door donations and there was no employee with the name she gave. Because my family member donated in cash the police said it would be difficult to locate this culprit, be careful out there!

And another close to home...

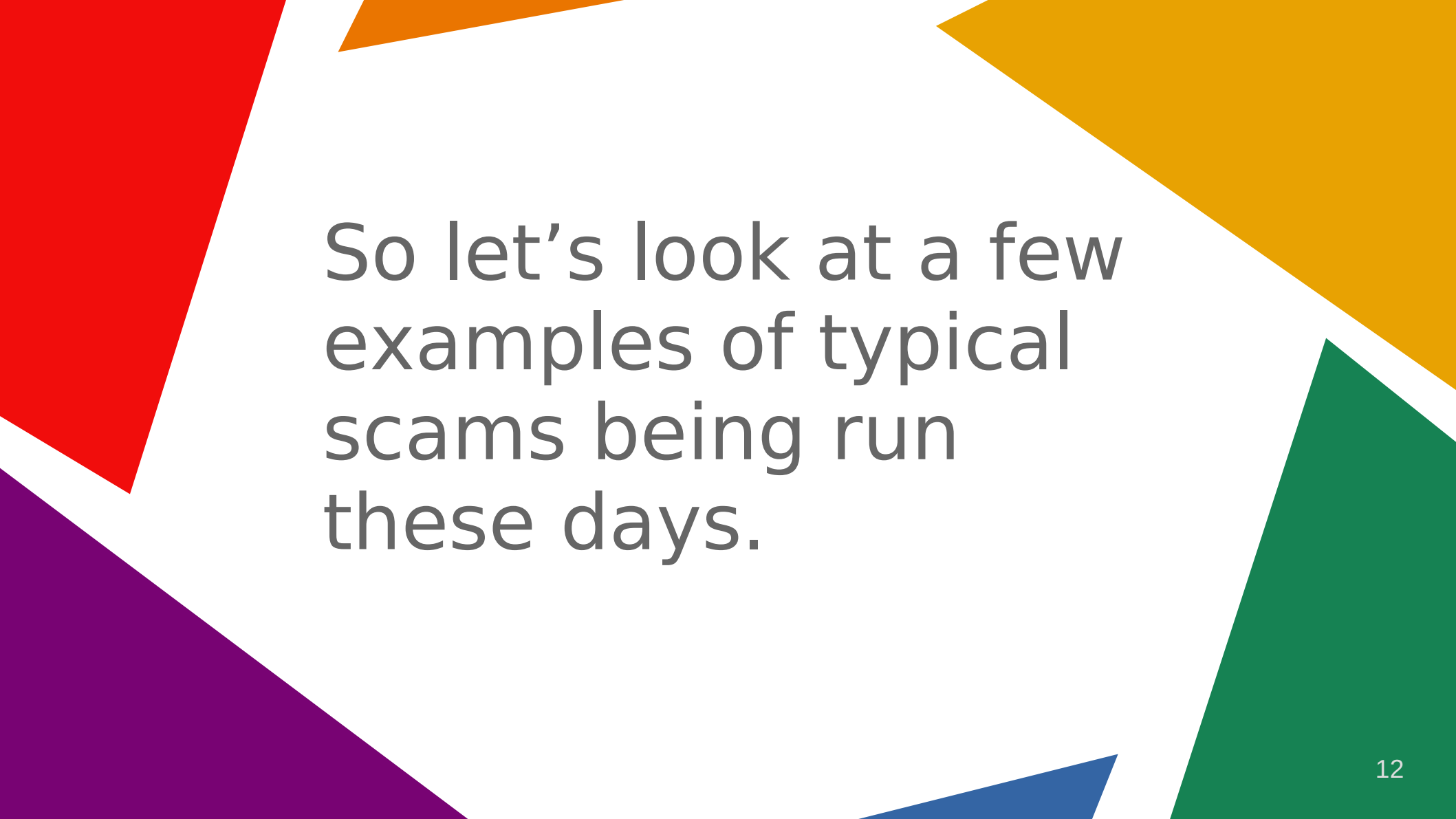
- <https://www.youtube.com/watch?v=jXRHb4sCM8c>

We of a certain age are prime targets

October 4, 2022 Press Release

- The Justice Department (DOJ) announced today that it would be accelerating its efforts to fight criminals who target older Americans for financial fraud. The new push will include adding 14 U.S. Attorney's Offices to the DOJ's Transnational Elder Fraud Strike Force — more than tripling the current number of offices, from six to 20.

- Other existing Strike Force members include the DOJ's Consumer Protection Branch, the FBI, the U.S. Postal Inspection Service and Homeland Security Investigations, which collaborate to fight elder fraud schemes.



So let's look at a few
examples of typical
scams being run
these days.

The mail scam...

- Thieves will snatch mail from residential mailboxes that have their flags up for pickup and/or will break into cluster-mailbox units at apartment or condo complexes.
- Criminals will get their hands on “arrow keys,” designed to open multiple mailboxes. Arrow keys are often stolen from mail carriers in what can be extremely violent robberies and are sold on the black market for \$5,000 to \$10,000.

- Thieves will then “wash” the stolen checks with a basic household chemical that can dissolve many kinds of ink. This allows them to make it out to whomever they want, change the dollar amount, and forge the customer signature from the check. Sometimes they even put some superglue over the signature of the check while washing it, to keep the original signature.

How to keep your mail secure

- Deposit mail in collection boxes as close to the indicated pickup time as possible — or take it to a post office for mailing.
- If you choose to leave outgoing mail in your mailbox, don't put up the flag.
- Try not to leave incoming or outgoing mail sitting in your mailbox for an extended time, particularly overnight.

- Sign up for Informed Delivery. This is a free service from the United States Post Office, and they will email you images of what will be delivered to your home that day. Over 44 million postal customers have signed up.
- Use the USPS Hold Mail service (you can sign up online) or have a neighbor collect your mail if you are going away for a time.

- Keep an eye on your bank accounts for potential fraud, and report suspicious activity as soon as possible.
- When making out a check, write out the amount — “One hundred and twenty dollars and ten cents,” for example — so the words fill out the line. This makes it more difficult for someone to wash off the ink. Also make sure the numeric amount fills the box on the far-right side of the check.

The phone is still #1 for scammers

- Scammers are good at getting targets to believe they are from a government agency or that they're a tech support provider, a retailer, or even a relative in distress.
- Criminals have long known the secret to their success is to play on our emotions. They will try to get you into a heightened emotional state — what they call “under the ether.” Once there, it's hard for us to think and we will believe just about anything.

- Typical ones are involving grandchildren or “you’ve just won!” Publishers Clearinghouse.
- Phone scams can often begin with a prerecorded robocall about some urgent matter that instructs you to stay on the line or press a button to speak to a representative.

Protect yourself from phone scammers...

- Use your voicemail or answering machine to screen incoming calls when you aren't absolutely certain who is calling. You can't trust caller ID because scammers use technology to hide their identity or make it look like a legitimate number.
- If the call induces a strong emotional response, pause and think.
- Plan ahead and think what you would do or say if you got such a call.

There are a lot of pet scams...

And here are some warning signs:

- Poor spelling and grammar in the ad.
- The asking price is far below the normal rate for a popular breed.
- The seller says the pet has to be shipped and won't allow you to collect it in person.
- The seller demands payment by money transfer, gift card or prepaid debit card.
- The shipment is continually held up by demands you wire more money for insurance, pet food, veterinary care or a special crate.

Pet scam protections...

- Research what reputable breeders are charging for the pet you're interested in. Be skeptical of deep discounts.
- Don't buy or adopt a pet unless you can meet it in person.
- Use a reverse-image search of pictures of the pet you are considering. Copy and paste text from the sales site or ad into a search engine. If you find matching images or text on multiple sites, you're probably dealing with a scammer.
- Don't deal with a seller who doesn't provide a phone number or will communicate only by email or text.
- Don't deal with someone who won't take payment by credit card, which offers you far greater protection in case of fraud or dispute.

- Do warn your grandkids. An unusually high proportion of victims of online pet scams are in their late teens or in their 20s.
- Check with the BBB to see if the person has been the subject of complaints. Check the seller's name against watchdog lists of suspected scammers.
- Don't believe threats that the animal will suffer or that you will face criminal charges if you don't continue sending money.
- Do consider adopting from a local shelter or rescue group, instead of buying a pet online. You can look up adoptable animals near you at Petfinder and the Shelter Pet Project.

Charity scams...

- While charity scams can happen at any time, they are especially prevalent after high-profile disasters like hurricanes or fires. Criminals often use tragedies to exploit you and others who want to help.
- Charity fraud scams can come to you in many forms: emails, social media posts, crowdfunding platforms, cold calls, etc. Always use caution and do your research when you're looking to donate to charitable causes.

- Check the website's address—most legitimate charity organization websites use .org not .com.
- Give to established charities whose work you trust but be sure it isn't scammers with copycat or similar names.
- Be wary of new organizations that claim to aid victims of recent high-profile disasters.
- Use a check or credit card. If a charity or organization asks you to donate through cash, gift card, virtual currency, or wire transfer, it's probably a scam.

- Use the Federal Trade Commission's resources to examine the track record of a charity.
- Do your research and decide which charities you want to support — before an event happens. You can check out charities online at [give.org](https://www.give.org) or [charitynavigator.org](https://www.charitynavigator.org)
- Make a list and stick to it. If you get a solicitation, simply say that you have made your giving decisions already.

Report charity fraud...

If you're a victim of charity or disaster fraud or you have info about these types of schemes, you can:

- Contact North Carolina's consumer protection office
- Report fraud to the FBI at tips.fbi.gov
- Report online fraud to the FBI's Internet Crime Complaint Center (IC3)
- File a complaint with the Federal Trade Commission (FTC)
- Report suspected disaster-related fraud to the National Center for Disaster Fraud

Other ways scammers can get you...

- Microsoft pop-up on your device saying it's detected a virus and provides a number for you to call immediately.
- Scammer are adept at making an email message look like it's coming from a trusted source, like your bank, and the goal is for the message to instill urgency, to get you to take an action (click a link, call a phone number) without stopping and thinking that maybe it's fraudulent.
- Text messaging is one of the fastest-growing contact methods these days. Like phone calls and emails, they impersonate a familiar or trusted source to get you to act immediately to address some urgent matter.

- There are a lot of legitimate-looking shopping sites online, and some are even fake versions of well-known retailers. Criminals buy ads that show up in web searches which lead you to a hot product at a great price. But clicking on the link lets them load malicious software onto your device which gives them access to usernames, passwords, etc. Always shop online with your “hand on your purse.”
- Be wary of “really good” deals or a “friend” pushing you to click on a link for some deal or little-known benefit.
- Be wary of friend requests from celebrities. Trust me. George Clooney doesn’t want to become your new BFF.

- Scammers will also use our impulse to stockpile limited supplies. They will allege there is a scarcity to convince us to act now, before it's too late.
- During the early months of the pandemic, fake ads for much-desired personal protective equipment, were rampant and then later it was about jumping the line to get the vaccine or quick access to in-demand testing.

Protections...

- **Make sure you enable updates on the operating systems of your desktop, laptop, smartphone and/or tablet whenever software patches are released. They can prevent known pathways of criminal activity. Also, be sure to use software to protect against computer viruses and keep it up to date. More on that later.**
- Be very careful If you use your device in public. It is recommended you not connect to free public Wi-Fi unless you enable a virtual private network (VPN). Options include ExpressVPN, NordVPN, Surfshark, etc.

“Federal Government” scams...

Here are some things the government does and doesn't do.

- The federal government will not call you unsolicited and ask for personal information. The agencies already have details like your Medicare and Social Security numbers.
- Any important communications from the federal government usually come via the US Postal Service.
- No federal government agency will initiate a serious contact with you through social media, text or email.

- The government won't reach out to offer you a federal grant. Grants require an application, and they are always for a specific purpose.
- No government office will ask you for an upfront payment before sending you a benefit, grant or refund.
- The government won't suspend benefits from Social Security or Medicare because someone else misused your identification. Federal law enforcement agents also won't bully you into revealing personal information such as your bank account number.

Protect your device...

- Windows and macOS have built-in firewalls. That is software designed to create a barrier between your information and the outside world. That's why you want those auto updates onto your system.
- Firewalls prevent unauthorized access to your device and alert you to any intrusion attempts. I personally recommend installing an antivirus software package.

Antivirus Software

There are a lot on the market to help protect your Windows 11 or Windows 10 computer. I found a rating list of the Best Antivirus Software of 2022.

The top five were:

- #1 Bitdefender
- #2 Norton
- #3 Kaspersky
- #4 ESET
- #5 Webroot

Macs can get viruses and other forms of malware although they are less common than on PC's. The built-in security features of macOS aren't enough to protect against all online threats. Best Mac antivirus software 2022:

- Intego Mac Internet Security X9.
- Clario Antivirus 1.5 for Mac.
- McAfee Total Protection.
- Norton 360 Deluxe.
- Avast Premium Security.

You have been victimized...

- If you have lost money or sensitive information, contact the police, tell them you are a victim of financial fraud and ask to file a report. Then file a report at reportfraud.ftc.gov. Though the chances of recovering losses is slim, your information will help investigators spot trends and possibly build cases.

Identity Fraud...

- Beyond stealing your money, some criminals specialize in stealing identities. Most of us have been notified that our sensitive information has been exposed in a data breach, which is a common way to steal identities. I suspect all of us have received notification from a company about such a breach.
- But identity theft can also involve stealing incoming or outgoing mail, going through garbage cans and recycling bins, or impersonating someone you would trust.

- Identity theft becomes identity fraud when someone uses your identity for financial gain, such as by opening new accounts in your name, filing for government benefits in your name, filing false tax returns — or even taking over your accounts.
- This fraud can be committed by the criminal who stole your data or by the criminal who bought your data.

Protection from identity fraud

- To protect yourself now against future identity fraud, add a fraud alert to your credit reports. This will require a lender to contact you before opening a new account in your name. Contact one of the three bureaus — Equifax, Experian or TransUnion — and the one you contact will alert the other two.
- Or you can freeze your credit. A freeze blocks lenders from opening new accounts in your name. You can freeze and unfreeze your reports at no cost, but you need to do it with each of the three bureaus.

- There are many steps consumers can take to minimize their risk of being an identity theft victim. For example, consumers should closely guard their social security number and shred charge receipts, copies of credit applications and other sensitive documents.
- Consumers also should review their bills and credit reports regularly and be aware of telltale signs to detect that their identity may have been stolen.

- If you find you have been victimized, there are a series of steps you can take to recover from identity theft and you need to do it as soon as you detect it. If you haven't already done it, place a credit freeze or fraud alert on your credit report and close accounts that may have been tampered with.
- Here's a helpful video: <https://www.youtube.com/watch?v=9DeOQmE55vA>

Sources to find out about scams...

- AARP is an excellent source. Search for “aarp fraud” on the Internet. They have a place where you can sign up for Biweekly Watchdog Alerts that come to you either by text or email (your choice).
- The FBI and the Federal Trade Commission also have things that can help you keep ahead of the scammers.

REMEMBER...

- The bad guys are smart and they change their schemes all the time, so you must be proactive.
- And I repeat once again as you need to get it into your brain: If something makes you laugh, sad, angry, or tugs at your heart strings, be suspicious. It may be something being used to manipulate you.

- Always
- **Stop,**
- **Relax, and**
- **Think**

The background consists of several large, overlapping triangles in various colors: red, orange, yellow, green, blue, and purple. The triangles are separated by thin white lines, creating a dynamic, geometric pattern.

Thanks for
coming...

January meeting
may be a
repeat.