

HOW CRIMINALS TARGET YOU

★ AND HOW TO STAY SAFE ★

- SLOW DOWN
- USE LOGIC, NOT EMOTION
- VERIFY BEFORE YOU TRUST

1 THEY STEAL YOUR DOCUMENTS

Mail theft, check fraud, and stolen information.

! THREATS



CHECK FRAUD

They steal or alter your checks left in your mailbox.



MAIL THEFT

They steal your mail.



DUMPSTER DIVING

They steal your trash.



HOW TO PROTECT YOURSELF



PROTECT YOUR CHECKS

- Pay electronically whenever possible.
- Use a gel pen to write your checks.
- Never leave checks in a mailbox for pickup.



PROTECT YOUR MAIL

- Sign-up for paperless delivery.
- Take outgoing mail inside the post office wherever possible.



PROTECT YOUR TRASH

- Shred sensitive documents with a micro-cut, diamond-cut, or cross-cut shredder.

2 THEY TEXT YOU

How criminals use texts to start scams.

! THREATS



EMOTIONAL TRICKS

They use fear, greed, curiosity to manipulate you.



AI-ENHANCED SCAMS

- Messages are more convincing and contain fewer mistakes.
- Criminals can personalize texts using information found online.
- All allows scammers to target thousands of people at once.



RANDOM OR "WRONG NUMBER" TEXTS

- "Wrong number" texts are often intentional, not accidental.
- They are designed to start a conversation and build trust over time.
- They are often the first step in an investment, romance, or cryptocurrency scam.



HOW TO PROTECT YOURSELF



PAUSE AND THINK

- Slow down—urgency is often a sign of a scam.
- Verify requests using a trusted phone number or website.
- Delete suspicious texts and block the sender.



DON'T LET AI FOOL YOU

- AI can make scam texts look professional and error-free.
- Be cautious of messages that create urgency or pressure you to act.
- Stop, verify, and think before taking action.



IGNORE UNEXPECTED TEXTS

- No good opportunity starts with a random or "wrong number" text.
- Delete and don't respond.
- Block the number if possible.



JEFF LANZA
Retired FBI
Special Agent



www.thelanzagroup.com



jefflanza@thelanzagroup.com

HOW CRIMINALS TARGET YOU ★ AND HOW TO STAY SAFE ★

● SLOW DOWN

● USE LOGIC, NOT EMOTION

● VERIFY BEFORE YOU TRUST

3 THEY EMAIL YOU

⚠ THREATS



OFFICIAL LOOKING EMAILS

- May appear legitimate, but are intended to steal your details.
- Criminals copy logos, commas, signatures, and branding to make emails appear legitimate.



DANGEROUS ATTACHMENTS

- May look like invoices, tax forms, or account documents.
- Designed to install malware on your computer or device.



FRAUDULENT LINKS

- May lead to fake websites that look real.
- Designed to steal usernames, passwords, and account information.



HOW TO PROTECT YOURSELF



DON'T PROVIDE INFORMATION

- Never provide personal, financial, or account information in response to unsolicited communications.
- Verify independently that an organization actually needs your information.



DON'T CLICK ON ATTACHMENTS

- Avoid attachments from unknown, suspicious, or unexpected senders.
- When in doubt, verify the sender before opening.



DON'T CLICK ON LINKS FROM UNKNOWN SENDERS

- Criminals can create fake websites that look identical to legitimate ones.
- Go directly to the organization's website or use its official app instead.

4 THEY PHONE IT IN

⚠ THREATS



VOICE CLONING

- AI can make their voice sound like someone you trust.



GRANDPARENT SCAMS

- They pretend to be a family member in urgent need of money.



TECH SUPPORT SCAMS

- They claim your computer, phone, or account has a serious problem.
- They convince victims to give remote access to their device.
- They demand payment through gift cards, cash, or cryptocurrency.



HOW TO PROTECT YOURSELF



VERIFY THE CALLER

- Don't trust caller ID—it can be faked.
- Hang up and call back using a number you know is real.



CREATE A FAMILY CODE WORD

- Set a secret word only family knows.
- Use the code word before sending money or sharing information.



HANG UP ON SCAMS

- Legitimate companies won't call you unexpectedly.
- Never give remote access to your computer to someone who contacted you first.



JEFF LANZA

Retired FBI
Special Agent



www.thelanzagroup.com



jefflanza@thelanzagroup.com

HOW CRIMINALS TARGET YOU ★ AND HOW TO STAY SAFE ★

- SLOW DOWN
- USE LOGIC, NOT EMOTION
- VERIFY BEFORE YOU TRUST

5 THEY HIJACK YOUR ACCOUNTS

Criminals take control to steal your money and information.

⚠ THREATS



WEAK OR REUSED PASSWORDS

Using a weak password or the same one on multiple accounts makes it easier for criminals to gain access.



FAKE LOGIN PAGES

Criminals create websites that look legitimate to steal your username and password.



ACCOUNT TAKEOVERS

Once inside, criminals can lock you out, reset passwords, access sensitive information, and steal money.



HOW TO PROTECT YOURSELF



UPGRADE YOUR PASSWORDS

- Use a passkey if a site allows it.
- Use passphrases or strong passwords as the next most secure option.
- Use a different one for every account.



VERIFY THE WEBSITE

- Check the web address before signing in.
- Use official websites and apps to log in, rather than a link that came in the message.



TURN ON MULTI-FACTOR AUTHENTICATION (MFA)

- Adds a second layer of protection.
- Helps stop account takeovers even if your password is stolen.
- MFA authenticator apps are more secure than text messages.

6 THEY IMPERSONATE

Criminals pretend to be someone or something you trust.

⚠ THREATS



GOVERNMENT IMPOSTERS

They pretend to be from a official government or law enforcement agency.



BANK IMPERSONATION SCAMS

They contact you and say there's a problem with your account.



ROMANCE SCAMS

They build trust over time before asking for money or financial help.



HOW TO PROTECT YOURSELF



COMMUNICATION WITH AGENCIES

- Government agencies do not demand immediate payment by gift card, cryptocurrency, wire transfer, or payment app.



CALL THE OFFICIAL NUMBER

- Don't use the number provided in the call or message.
- Look up the bank's number on their official website.



MONEY REQUESTS ARE A WARNING SIGN

- If they ask for money, it's a scam—100% of the time.
- Never send money to someone you have not met in person.
- Talk to a trusted friend or family member before sending money.



JEFF LANZA
Retired FBI
Special Agent



www.thelanzagroup.com



jefflanza@thelanzagroup.com

SIX TIPS ★ TO STAY SAFE ★

Six additional ways to stay protected.

1



**FREEZE YOUR
CREDIT REPORTS**



Make it harder for criminals to open new accounts in your name.

2



**CREATE AN ONLINE
SOCIAL SECURITY
ACCOUNT**



Prevents criminals from setting up a Social Security account using your identity and having your benefits sent to them.

3



**KEEP YOUR
SOFTWARE
UP TO DATE**



Keep your devices, apps, browser, and antivirus software up to date.

4



**ONLY UNSUBSCRIBE
FROM SENDERS
YOU TRUST**



Unsubscribing from spam can confirm your email is active and increase scam risk.

5



**PREVENT SIM
CARD SWAPPING**



Set up a passcode with your cell phone provider to prevent anyone from making changes to your account.

6



**YOUR PASSWORD
UPGRADE**



PASSKEYS (BEST)

Use passkeys for accounts that allow it.

PASSPHRASES (NEXT BEST)

Use passphrases as the second best secure option.

STRONG PASSWORDS

Use strong passwords that are long and complicated.



SLOW DOWN



**USE LOGIC,
NOT EMOTION**



**VERIFY BEFORE
YOU TRUST**



**Most scams succeed because criminals create urgency and emotion.
Slow down. Use logic. Verify before you trust.**



JEFF LANZA
Retired FBI
Special Agent



www.thelanzagroup.com



jefflanza@thelanzagroup.com

CYBERCRIME QUICK REFERENCE GUIDE

★ IMPORTANT CONTACTS & WHAT TO DO ★



IMPORTANT CONTACTS

REPORT FRAUD OR IDENTITY THEFT



FBI Internet Crime Complaint Center (IC3)

Report online scams, wire fraud, romance scams, investment scams, ransomware, and account takeovers.

ic3.gov



Federal Trade Commission (FTC)

Report fraud and identity theft.

IdentityTheft.gov
ReportFraud.ftc.gov



Social Security Administration

Create and monitor your online Social Security account.

ssa.gov



IRS Identity Protection

Tax-related identity theft and fraud.

irs.gov/identity-theft



U.S. Postal Inspection Service

Report mail theft, check fraud, and other postal crimes.

postalinspectors.uspis.gov



Your State Attorney General

Report scams and get consumer protection help.

Find at: naag.org



AARP Fraud Watch Network

Get help and resources for avoiding scams.

aarp.org/fraudwatchnetwork
1-877-908-3360

CREDIT REPORTS – FREEZE YOUR CREDIT



Experian

experian.com/freeze
1-888-397-3742



Equifax

equifax.com/freeze
1-888-298-0045



TransUnion

transunion.com/freeze
1-888-909-8872



Innovis

innovis.com/freeze
1-800-540-2505

Freezing your credit makes it harder for identity thieves to open new accounts in your name.



IF THIS HAPPENS, DO THIS



IF SOMEONE GETS INTO YOUR EMAIL

- ✓ Change your password immediately.
- ✓ Turn on multi-factor authentication (MFA).
- ✓ Review account recovery settings.
- ✓ Check sent and deleted folders.
- ✓ Notify important contacts.



IF YOU CLICKED A SUSPICIOUS LINK

- ✓ Change affected passwords.
- ✓ Run security software scan.
- ✓ Monitor financial accounts for unusual activity.
- ✓ Contact your bank if financial information was entered.



IF YOUR IDENTITY IS STOLEN

- ✓ Freeze your credit reports.
- ✓ Report at IdentityTheft.gov.
- ✓ Monitor accounts and statements closely.
- ✓ Change compromised passwords.
- ✓ Keep a record of everything.



IF YOU SENT MONEY TO A SCAMMER

- ✓ Contact your bank immediately.
- ✓ Request a wire recall if applicable.
- ✓ Report to [IC3.gov](https://ic3.gov).
- ✓ Save all communications and receipts.

Time matters—act immediately.



IF YOU RECEIVE A CALL CLAIMING TO BE:



THE FBI



IRS



SOCIAL SECURITY



LOCAL POLICE



YOUR BANK

- ✓ Hang up.
- ✓ Find the official number yourself.
- ✓ Call back using that number.



Real agencies will never demand payment or threaten you.



IF YOU THINK YOUR PHONE NUMBER WAS STOLEN (SIM SWAP)

- ✓ Contact your mobile carrier immediately.
- ✓ Request a SIM card block.
- ✓ Change important passwords.
- ✓ Review financial accounts for unauthorized activity.



DON'T LET EMOTIONS DRIVE YOUR DECISION-MAKING



REMEMBER



SLOW DOWN



VERIFY BEFORE YOU TRUST



For more information and prevention tips, visit www.lanzagroup.com



jefflanza@thelanzagroup.com

Presented by Jeff Lanza
Retired FBI Special Agent