Identity Theft

Lesson 6: Teacher's Guide | Hall of Fame: Ages 18+

FINANCIAL FOOTBALL

Avoiding Injury with Identity Theft Protection

Identity theft protection and fraud prevention are incredibly important aspects of a healthy financial life. This 45-minute module empowers students to manage risks, monitor their financial lives, and take preventive action to protect their financial futures.

Getting Your Class Game-Ready: Training players has many benefits. It builds strength and agility, it provides time for practice and growth, and it helps minimize the risk of injury. Players work diligently to protect themselves on and off the field.

While most of us are not dodging tackles at high speeds, we do have a similar need to protect ourselves when it comes to finances. Identity theft has become increasingly prevalent and even affects children before they start building their own credit. Being aware of common risks and prevention strategies is an important step students can take to protect their identities.

Module Level: Hall of Fame, Ages 18+

Time Outline: 45 minutes total

Subjects: Economics, Math, Finance, Consumer Sciences, Life Skills

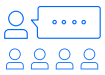
Materials: Facilitators may print and photocopy handouts and quizzes for students, or direct them to the online resources below.

- **Pre- and Post-Test questions:** Use this short grouping of questions as a quick, formative assessment with the Identity Theft module or as a Pre- and Post-Test at the beginning and completion of the entire module series.
- **Practical Money Skills Identity Theft resources:** practicalmoneyskills.com/ff43
- **Identity Theft Game Plan activity handout:** Using the research tools provided, students will brainstorm and create a list of strategies to build awareness, prevent problems, and protect themselves from identity theft.
- **Two Scams and an Ad handout:** Students can play with a partner or small team to see how many identity theft risks they can identify.
- **Glossary of Terms:** Students learn basic financial concepts with this list of terms.

Icon Key

Activity

Assign the given activity to students and have them complete it individually or with a group, depending on the instructions.



Ask

Pose questions to your students and have them respond.

Assign

Designate individuals or groups to complete a particular assignment.

Debrief

Examine the activities as a whole group and compare answers and findings.

Did You Know?

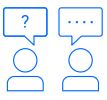
Share these fun facts with students throughout the lesson.

Pre- and Post-Test

Have students take the Pre-Test before the lesson, and take the Post-Test after completing the lesson.

Share

Read or paraphrase the lesson content to students.



Turn and Talk

Have students turn to a partner and discuss a specific topic or question.

Table of Contents

Learning Objectives

– Identify what identity theft and fraud are and how they can impact students' financial lives
– Examine strategies to avoid identity theft and scams
– Discover ways to handle identity theft, fraud, and/or security breaches

Key Terms and Concepts

Before you start the lesson, review the key terms and concepts below. The answers to each question will help you get students prepped and game-ready. Get deeper information around these concepts in the Facilitator Script section of this guide on pages 6 to 9 of this guide.

What is identity theft?

Identity theft can take many forms. With financial identity theft, it's often a case of bank accounts or credit cards being accessed and used illegally. For example, the thief may take out cash or max out a credit card. Uncaught it can have a serious impact on your credit score. Another form of identity theft is when criminals gain access to your Social Security number and use it illegally — to take out loans or open credit card accounts, for example.

What are common types of identity theft scams?

- **Phishing:** This refers to scams that attempt to trick consumers into revealing their personal information such as bank account numbers, passwords, payment card numbers, or insurance account numbers.
- **Emails:** Be aware that emails coming from suspicious sources may be attempts to access your personal financial information. Do not reveal your financial account passwords, PINs, or other security-based data to third parties; genuine organizations or institutions do not need your secret data for ordinary business transactions.
- **Smishing:** Smishing is similar to a phishing scam. Computer users receive an authentic-looking email that appears to be from their bank, Internet service provider (ISP), favorite store, or some other organization. Smishing messages are also sent to you via SMS (text message) on your mobile phone. Do not respond to them. Delete them and the emails.
- **Clone Phishing:** This refers to resending an email that now has a malicious attachment or link. Do not open attachments to questionable emails; they may contain viruses that will infect your computer.
- **Vishing:** Vishing is where a scammer calls you pretending to be someone you know in the attempt to get your personal financial information. Potential victims may hear an automated recording informing them that their bank account has been compromised and providing a toll-free number to reset security settings associated with the account.
- **Skimmers:** This is when scammers install devices at an ATM, a gas station pump, or a store's checkout counter to copy the information from your debit or credit card.
- **Whaling:** These scams are directed at high-profile business individuals to get their personal financial information.
- **Doxing:** Doxing scams occur when someone releases online personal information about their victim, like their home address or cellphone number. Short for 'dropping docs,' it is a tactic hackers use to breach someone's personal data and publish it online as a means of harassment.

Key Terms and Concepts, cont.

What steps can I take to protect myself from identity theft?

There are six simple steps students can take to reduce the risk of becoming a victim of identity theft or card fraud.

1. Practice safe internet use
2. Destroy unneeded financial documents
3. Guard your Social Security number
4. Check your credit report
5. Beware of scams
6. Secure your mail

Did You Know?

Secure Sockets Layer (SSL) is data protocol used to keep your online transactions safe. Some URLs start with "http://" while others start with "https://". Did you notice that extra "s" when you were browsing websites that require giving over sensitive information, like when you were paying bills online? The extra "s" means your connection to that website is secure and encrypted, and any data you enter is safely shared with that website.

What do I do if I think I have been a victim of identity theft?

If private financial information gets into the wrong hands, the consequences can be devastating. If students find themselves victims of identity theft, they should act quickly, taking the following steps:

- Report the fraud to your bank or credit union that issued the card and request replacement cards
- Report the fraud to law enforcement
- Contact the fraud departments of each of the credit bureaus
- File a fraud report
- Create a fraud recovery plan

Where can I get help and information about identity theft?

For information about fighting back against identity theft, visit the FTC's Identity Theft website (identitytheft.gov) or call the hotline: 1-877-IDTHEFT (1-877-438-4338).

Credit Bureau Contact Information

Equifax
Order Credit Report: 1-800-685-1111
Fraud Hotline: 1-888-766-0008
equifax.com

Experian
Order Credit Report: 1-888-397-3742
Fraud Hotline: 1-888-397-3742
experian.com

TransUnion
Order Credit Report: 1-877-322-8228
Fraud Hotline: 1-800-680-7289
transunion.com

Module Section Outline with Facilitator Script

Introduction: Warm-Up

Ask: Pose the following question to students: what is identity theft?

Share: Explain to students that it's a growing problem impacting millions of Americans and 3% of children ages 19 and under according to the Federal Trade Commission.[1] Identity theft can take many forms. With financial identity theft, it's often a case of bank accounts or credit cards being accessed and used illegally. For example, the thief may take out cash or max out a credit card. This can have a serious impact on your credit score. Another form of identity theft is when criminals gain access to your Social Security Number and use it illegally — to take out loans or open credit card accounts, for example. Tell students that you will explore what it can look like and how it can be avoided.

Turn and Talk: Have students turn to a partner and suggest one way you might avoid identity theft.

Optional Pre-Test: Have students turn to page 6 of their Student Activities guide.

Identity Theft Basics

Share: Reinforce to students that there are many types of identity theft associated with your financial information. Here are a few common types of scams.

- **Phishing** refers to scams that attempt to trick consumers into revealing their personal information such as bank account numbers, passwords, payment card numbers, or insurance account numbers.

Did You Know?

Online phishing scams typically ask for personal information like your mother's maiden name and your date of birth.

- **Emails** that come from suspicious sources can be attempts to access your personal financial information. Do not reveal your financial account passwords, PINs, or other security-based data to third parties; genuine organizations or institutions do not need your secret data for ordinary business transactions. If you think you have received a fraudulent email, contact your financial institution immediately.
- **Smishing** is similar to a phishing scam. Computer users receive an authentic-looking email that appears to be from their bank, Internet service provider (ISP), favorite store, or some other organization. Smishing messages are also sent to you via SMS (text message) on your mobile phone. Do not respond to them. Delete them and the emails. Victims prompted by a text message that looks like it is from their bank, telling them to respond to an emergency by providing their personal financial information.
- **Clone Phishing** is resending an email that now has a malicious attachment or link. Do not open attachments to questionable emails; they may contain viruses that will infect your computer.

Module Section Outline with Facilitator Script, cont.

- **Vishing** is where a scammer calls you pretending to be someone you know in an attempt to get your personal financial information. Potential victims may hear an automated recording informing them that their bank account has been compromised and providing a toll-free number to reset security settings associated with the account.
- **Skimmers** are devices fraudsters install at an ATM, a gas station pump, or a store's checkout counter to copy the information from your debit or credit card.
- **Whaling** scams are directed at high-profile business individuals to get their personal financial information.
- **Doxing:** Doxing scams occur when someone releases online personal information about their victim, like their home address or cellphone number. Short for 'dropping docs,' it is a tactic hackers use to breach someone's personal data and publish it online as a means of harassment.

Preventing Fraud

Share: Being aware of common risks and prevention strategies is an important step in protecting your identity. There are six simple steps students can take to reduce the risk of becoming a victim of identity theft or card fraud.

1. Practice Safe Internet Use

Delete spam emails that ask for personal information, and keep your antivirus and anti-spyware software up-to-date. Shop online only with secure web pages (check the address bar for "https" next to an image of a lock). Never email credit card numbers, Social Security numbers, or other personal information. Research mobile app privacy policies before downloading and allowing them access to your social media accounts.

Did You Know?

To reduce the risk of identity theft while shopping online, only order from secure sites that begin with "https://"

2. Destroy Unneeded Personal Financial Records

Shred unneeded credit card statements, ATM and debit card receipts, and other documents that contain personal financial information.

3. Guard Your Social Security Number

Thieves seek your Social Security number because it can help them access your credit and open bogus accounts. Never carry your card; instead, memorize your number and store the card securely.

4. Check Your Credit Report

Regularly review your credit reports for suspicious activity. You can request one free copy of each report per year at annualcreditreport.com or contact the three credit bureaus directly. If you are suddenly denied credit for no apparent reason, this could indicate credit fraud.

5. Beware of Scams

Never give out personal information via phone or email to someone claiming to represent your bank, a

Module Section Outline with Facilitator Script, cont.

credit card company, a government agency, a charity, or any other organization. If you think the request is legitimate, contact the company directly to confirm it.

6. Secure Your Mail

Empty your mailbox regularly and consider investing in a mailbox lock. When mailing bill payments and checks, consider dropping them off at the post office or in a secure mailbox.

Did You Know?

One indicator of being a victim of identity theft is that your credit report shows unfamiliar activity.

Share: Explain to students that, in order to build their agility and learn to protect their information, they'll work in teams to create a game plan. Break students into small groups. Each group will research and document things to watch out for (awareness), things to avoid (prevention), and things to do (protection) to prevent identity theft, based on the focus areas below. Refer them to the Identity Theft Protection Game Plan on page 7 of their Student Activities guide.

Assign: Direct each group to focus on one of the areas below as they open the Identity Theft Protection Game Plan on page 7 of their Student Activities guide. You may have more than one group working on each of the focus areas.

- Protecting yourself online
- Protecting yourself in real life while out and about
- Protecting yourself at home and on your devices
- Protecting yourself during travel
- Protecting yourself while banking

Debrief: Following the activity, examine the game plans you created as a whole group; add any strategies the group may have missed using the Answer Key on pages 14 to 15 of this guide.

Share: Explain that many people choose to freeze their credit after actual or suspected fraud, as well as to use credit monitoring services, which work by alerting you to warning signs on your accounts.

Putting It Into Practice

Activity: Refer students to the Two Scams and an Ad activity on page 9 of their Student Activities guide. It should be played like two truths and a lie. There are two options for game-play:

Option 1: Have students play in partners or small groups to evaluate calls, emails, and marketing materials described in the Two Scams and an Ad handout and determine whether the scenario is a scam.
Option 2: Play vote with your feet. Read an option aloud and have students who believe it is a scam stand and move to the right side of the room. Students who do not believe it is a scam should stand and move to the left side of the room.

Module Section Outline with Facilitator Script, cont.

Getting Help If You Need It

Share: Tell students that there are key things to consider when you're worried about potential identity theft, fraud, and/or security breaches. If your private financial information gets into the wrong hands, the consequences can be devastating. Let your parents know if you're receiving spam, phishing emails, unwanted calls or texts, or notice a purchase on your account that you didn't make. If you find yourself a victim of identity theft, act quickly and contact law enforcement and the credit reporting companies.

Report the fraud to law enforcement.
Report identity theft to your local police department. If the crime occurred somewhere other than where you live, you may want to report it to law enforcement there as well. The police will create an "identity theft report" and you can request a copy.

Contact the credit reporting companies.
Immediately contact the fraud departments of each of the credit bureaus. Alert them that you have been a victim of identity theft, and request that a fraud alert be placed in your file. You can also request a security freeze, preventing credit issuers from obtaining access to your credit files without your permission. This prevents thieves from opening new credit cards in your name.

File a fraud report.
The Federal Trade Commission (FTC) does not investigate identity theft cases, but it can share information that you provide, such as the identity theft report number, with investigators nationwide. For more information about fighting back against identity theft, visit the FTC's Identity Theft website or call the hotline: 1-877-IDTHEFT (1-877-438-4338).

Create a fraud recovery plan.
The Federal Trade Commission can help you create a recovery plan if you've become a victim of identity theft. When you report what happened, you'll receive a personalized recovery plan and can track your progress online step-by-step. Learn more at identitytheft.gov.

Closing: Group

Ask students: what key tip they would give a friend about preventing identity theft and fraud.

Discussion

Optional Post-Test: Direct students to take the test on page 6 of their Student Activities guide.

Get more information on identity theft

- Learn more about identity theft basics and ways to protect yourself at practicalmoneyskills.com/ff43
- Read the Identity Theft Practical Money Guide at practicalmoneyskills.com/ff45

Lesson 6 Identity Theft: Answer Keys

> Identity Theft Protection Pre- and Post-Test

> Identity Theft Protection Game Plan

> Identity Theft Protection: Two Scams and an Ad

Identity Theft Protection Pre- and Post-Test

Directions: Direct students to open the test on page 6 of their Student Activities guide. Have them answer the questions with the most appropriate answer, noting a, b, c, d or filling in the blank.

Answer Key

1. Which is an effective way to prevent fraud?

a. Shredding documents that contain credit account information

b. Online shopping only on secure sites

c. Spreading purchases over various accounts

d. Both A and B

2. An indicator that you've been a victim of identity theft could be:

a. Getting a prank call

b. Your bank adding additional security measures to its site

c. Denials of credit for no apparent reason

d. You meet someone with the same name as you

3. To reduce the risk of identity theft:

a. Shred mail with personal information

b. Photocopy credit cards and keep copies in a safe place

c. Share your credit card number only when making purchases

d. All of the above

4. What are examples of safe internet use?

(Possible answers: Delete spam emails that ask for personal information, keep your antivirus and anti-spyware software up to date, or shop online only with secure web pages)

5. What are warnings signs to watch out for scams?

(Possible answers: checks or bills from organizations you don't recognize, spam emails)

Identity Theft Protection Game Plan

Answer Key

Identity theft is a growing problem that causes financial damage to millions of Americans. To lower your chances of becoming a victim of identity theft, it's important to understand how to best protect your finances and personal information.

Directions: Each group will research and document things to watch out for (awareness), things to avoid (prevention) and things to do (protection) in order to protect themselves. It's time to get students started on creating their game plan. Divide them into teams and have them select or assign a group focus from one of the options below from page 7 of their Student Activities guide. Allow them time to research their topic before they write their list of strategies to build awareness, prevent problems, and protect themselves from identity theft.

Have Students Select Group's Research Focus (Check One of the Boxes Below)

☐ Protecting yourself online

☐ Protecting yourself in real life and out and about

☐ Protecting yourself at home and on your devices

☐ Protecting yourself when you travel

☐ Protecting yourself while banking

Create a Plan

Have students use the research resources below and ask for their team's ideas to create a list of strategies to build awareness, prevent problems, and protect themselves.

- Identity Theft Basics: practicalmoneyskills.com/ff46
- How to Prevent Fraud: practicalmoneyskills.com/ff47
- Identity Protection While Traveling: practicalmoneyskills.com/ff48
- CFPB Fraud and Scams: consumerfinance.gov/consumer-tools/fraud/

Build Awareness

What warning signs should people watch out for when it comes to fraud or identity theft?

Identity Theft Protection Game Plan, cont.

Possible Answers:

- *Receiving collection calls or bills for services you didn't use*
- *Phishing emails asking for your personal information (consider who this is, what they are asking, and why)*
- *Apps asking for access to your social media accounts*
- *Phone calls asking for money so you can get a gift or service you didn't seek out*
- *Sales people offering "today only" deals and pressuring you to act now*

Prevent Possible Problems

What risks should people avoid taking with regards to their information?

Possible Answers:

- *Don't share passwords, account credentials, or PINs*
- *Don't pay up front for a promised gift/prize from unknown source*
- *Don't leave sensitive documents in unsecured or public places*
- *Avoid using unsecured public Wi-Fi when accessing sensitive information such as in online banking*
- *Don't open emails, text links, or social media messages that are from anyone you don't recognize and cannot authenticate*
- *Consider how you pay: some methods like online services or wiring money are riskier than others*

Protect Yourself

What actions can you take to protect your information?

Possible Answers:

- *Practice safe internet use: delete spam emails, keep antivirus and antispam software up-to-date*
- *Only shop online at secure locations (look for https:// in address bar)*
- *Destroy private records, including things like old ATM, credit, debit card receipts*
- *Use privacy settings in apps and on websites*
- *Use tough passwords and change them regularly*
- *Secure your mail, empty your mailbox regularly*
- *Monitor your accounts (email, social media, cell phone, and banking) for suspicious activity*
- *Do online searches to vet information*

Identity Theft Protection: Two Scams and an Ad

Directions: Can your students spot the scam? Have them play with a partner or small team to see how many risks they can identify. Their answer should identify each scenario as a "scam" or an "ad" and explain their reason why. They should include tips or best practices for protecting their identity against this type of fraud.

Something Phishy

1. You get a call and are excited to hear you've been awarded a scholarship! They know your name, your school, and when you're graduating. They say that, in order to finalize the award, they will need your address and banking details.

   Answer: *Scam; a valid scholarship offer will not require you to provide banking information over the phone. Ask yourself: Who is calling? What are they asking for and why? Do a web search to see if you can find other verifying information.*

2. You get a text from a store you've only gone to once offering 50% off. The text includes a link to the national website to download the offer.

   Answer: *Most likely an ad, if this is a recognizable store and website.*

3. You get an email invite to view a cloud-based document; it's your friend's name but the email isn't one you remember your friend using.

   Answer: *Scam; avoid opening links you do not recognize. It might install malware or phish your information.*

Mal Intent or Just Annoying Marketing?

1. You get a text with a brief survey from your favorite store two days after making a purchase there. You told the sales clerk you didn't want text offers.

   Answer: *Most likely an ad.*

2. Someone knocks on the door, selling magazines for a school fundraiser. For just $5 you can get two years of your favorite subscription. They need you to give your name, address, and credit card info. They offer a glossy handout listing the magazines but no other formal documentation.

   Answer: *Scam; avoid giving financial information to contacts you cannot validate.*

3. You get a text offering help to get scholarships; it says "Click here to sign up today for discounted access to support."

   Answer: *Scam; avoid opening links you do not recognize. It might install malware or phish your information.*

Identity Theft Protection: Two Scams and an Ad, cont.

Unexpected Sharing or Serious Issue?

1. You shared a video online explaining the solution to a math problem. The video did not show your face, just the math problem close up onscreen. Someone commented on the video, sharing your name, phone number, and email and telling others they should reach out for tutoring.

Answer: *Scam/Identity Theft Risk: This practice of sharing personal information without the person's permission is called doxing and can cause serious problems. Delete the video as soon as possible so the comments sharing your personal information are removed.*

2. You download an app and it asks if it can access your personal information.

Answer: *Most likely an ad, but it's important to protect your privacy and limit apps' access to your personal information. Consider not allowing all apps access to your camera, microphone, and GPS.*

3. Your friends shared an online quiz; it's easy to take and the results tell you which of your favorite TV characters you are most like. When you click on the link through social media, it requires access to your profile and asks permission to post your result to your profile.

Answer: *Identity Theft Risk: While not always scams, online quizzes from random sites and apps that require access to your social media profile may allow access to your social media account info in order to track future behavior. Consider reading the fine print or limiting what you share with third parties.*

Convenience or Con?

1. You're at a street festival with friends and decide to buy a few things at one of the booths. The person at the booth says the card scanner is in back and asks for your card, promising to be right back.

Answer: *Identity Theft Risk: Credit card skimming either with a digital scanner or by photographing card details can result in fraudulent charges.*

2. You're running errands with your family and someone notices the credit card reader at the gas station looks different and is sticking out slightly. Seems odd, but it looks like the machine is working.

Answer: *Identity Theft Risk: Credit card skimming with a digital reader happens often at gas pumps. Before you swipe, check to make sure the seal around the card reader is not broken; wiggle the card reader to make sure it's firmly in place. Stick to using pumps that are out in the open.*

3. You're at the grocery store, and after you swipe your debit card, the checker offers you a game board and stickers so you can start playing the grocery sweepstakes game.

Answer: *Most likely an ad, if this is a familiar store and they have marketing materials showing the sweepstakes.*

Identity Theft Protection: Two Scams and an Ad, cont.

Summer Job or Position in Pyramid Scheme Scam?

1. Several friends are working as dog walkers using a new app. It lets pet owners see days you are available to work and lets you set your own rate. You mention wanting to try it and a friend sends you an invite through the app.

Answer: *An ad. This is a common way app marketing info gets shared. Just make sure you recognize who invited you before accepting and sharing personal info.*

2. You're scrolling on a social media site when you spot a friend's meme: "Need some extra cash? Turn $5 into $40… Join my team and download the cash app below."

Answer: *Scam: Be very cautious of social media posts that promise to grow your money by downloading and sharing new apps or grow teams to pool/crowdfund money. These are pyramid schemes.*

3. You see a flyer out in front of a local coffee shop; "Summer job, work at home, do crafts for easy money." It includes a phone number and website. Curious, you check out the website info and see it costs $49.99 to get a starter kit of high-quality supplies.

Answer: *Scam: Be wary of any job offer that asks for money up front for training or supplies. Many pyramid schemes start this way.*

Banking Bonus or Big Red Flag

1. You've been traveling and get a phone call from an unrecognized number. They say they are from your bank and noticed an odd charge on your account. They need you to verify your account information before they can tell you more.

Answer: *Scam: your bank will not ask you to share all of your account information over the phone. When in doubt, hang up and call your financial institution using the toll-free customer service phone number on the back of your debit or credit card.*

2. You're at your local bank and the teller shares that they have a special promotion going: if you open a new savings account with a minimum balance of $1,500, they will give you one of the stuffed animals on display and a $50 credit to your new account.

Answer: *Ad: this is a common practice for getting customers to consider new services.*

3. You're reading through emails and come across one from your bank; when you open it you notice the address it was sent from is slightly misspelled. It states you need to confirm your address for bank statements. Curious, you click the link and it looks like your bank website.

Answer: *Scam: watch out for warning signs of phishing emails including incorrect emails, misspellings, and links to fake websites.*

Glossary of Terms

Have students study this list of personal finance terms to warm up before playing Financial Football. By mastering these terms, students will have a better opportunity to answer questions in the game correctly and score.

Clone Phishing: This is resending an email that now has a malicious attachment or link. Do not open attachments to questionable emails; they may contain viruses that will infect your computer.

Credit bureau: A credit bureau is a company that gathers and stores various types of information about you and your financial accounts and history. They use this information to create your credit reports and credit scores. The three major consumer credit bureaus are Equifax®, Experian®, and TransUnion®.

Doxing: Doxing scams occur when someone releases online personal information about their victim, like their home address or cellphone number. Short for 'dropping docs,' it is a tactic hackers use to breach someone's personal data and publish it online as a means of harassment.

Identity theft: The fraudulent use of another person's information for financial gain.

Malware: Software that is intended to damage or disable computers and computer systems.

Pharming: The fraudulent practice of directing internet users to a bogus website that mimics the appearance of a legitimate one, in order to obtain personal financial information such as passwords, account numbers, etc.

Phishing: The fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal financial information, such as passwords and credit card numbers.

Pyramid schemes: Illegal schemes in which money from new investors is used to show a false return to other investors.

Scam: A fraudulent activity or deceptive act.

Security breaches: An incident that results in unauthorized access of data, applications, services, networks, and/or devices by bypassing their underlying security mechanisms.

Skimming: A method used by identity thieves to capture information from a card holder.

Smishing: This is similar to a phishing scam. Computer users receive an authentic-looking email that appears to be from their bank, Internet service provider (ISP), favorite store, or some other organization. Smishing messages are also sent to you via SMS (text message) on your mobile phone. Do not respond to them. Delete them and the emails.

Social Security identity theft: A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, if they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Find out more at ssa.gov/pubs/EN-05-10064.pdf

Whaling: These scams are directed at high-profile business individuals to get their personal financial information.