

# How to Be #UnHackable

*Learn to Think Like a Scammer to Improve Your Cybersafety Skills*



**Facilitated by:**

**Claudiu Popa, Founder**  
**Debra Popa, Executive Director**

# KnowledgeFlow Cybersafety Foundation

Making Canadians  
#UnHackable.



KnowledgeFlow.org



This Hour Has 22 Minutes

55 minutes ago

Don't touch that dial!



**An Ottawa couple is out 13K after a scammer posing as TD bank stole their credit card info.**

**Authorities are advising people to straight up never answer the phone ever again.**

## What Do We Know About Fraud?



**Claudiu Popa, CISSP, CISA, CIPP, CRISC, PMP**

Founder

KnowledgeFlow Cybersecurity Foundation



**Debra Popa, MBA**

Executive Director

KnowledgeFlow Cybersecurity Foundation

# KnowledgeFlow.org/Events

- View and download your handouts
- Complete the survey



The screenshot shows the KnowledgeFlow.org website with a navigation bar containing links for About Us, Resources, Initiatives, Solutions, Cyber Hub, Events (highlighted), Blog, and Contact. The main content area features a webinar announcement for November 19th, 2024, titled "How To Be #UnHackable: Learn To Think Like A Scammer To Improve Your Cybersafety Skills". Below the title is a description of the webinar, an image of a man and a woman, and two call-to-action buttons: "View Materials" and "Open Survey".

**KNOWLEDGEFLOW** About Us Resources ▾ Initiatives Solutions Cyber Hub ▾ **Events** Blog

## Cybersafety Webinar | November 19th 2024

November 19 📺 Virtual Event

### How To Be #UnHackable: Learn To Think Like A Scammer To Improve Your Cybersafety Skills

Join our upcoming webinar, "How to Be #UnHackable: Learn to Think Like a Scammer to Improve Your Cybersafety Skills" with KnowledgeFlow Cybersafety Foundation. We will be introducing KnowledgeNet and KnowledgeLink, two ground-breaking initiatives designed to protect seniors in the digital world. Learn how KnowledgeNet uses real-life scenarios to empower seniors to recognize and prevent online fraud, while KnowledgeLink builds a supportive network of senior ambassadors who help peers navigate cybersafety confidently. We'll also cover essential cybersafety tips for seniors and highlight the ways KnowledgeFlow promotes digital literacy and online safety for all ages. Don't miss this chance to enhance your knowledge and protect yourself online!



**Participant Materials**

Download your certificate and handouts here. Thank you for attending!

[View Materials](#)

**Participant Survey**

Please take a moment to provide us with some feedback on the event. Thank you.

[Open Survey](#)

# Project KnowledgeNet



## Designed by seniors for seniors:

- the goal is to improve senior cybersafety in all aspects daily life



## Interactive scam spotting email course:

- receive phishing scam simulation emails—training you to recognize real ones and stay safe online



## Cybersafety for Everyone:

- a free online course teaching a thorough overview of personal cybersafety

# Project KnowledgeNet: How to Sign Up

- **KnowledgeNet.KnowledgeFlow.org**



**Register to join our Interactive Scam Spotting Email Course**


Throughout our Scam Spotting Email Course, we will be sending you harmless phishing simulations to your inbox to test your ability to spot them. Additionally, you will receive educational emails breaking down these simulations and helping you learn what red flags you might have missed. This course is designed to improve your scam-spotting skills in a fun and interactive way. Enter your email below to join the course!

Email Address:

First Name:

Last Name:

[Join Now](#)



## You've Been Caught In Our Phishing Net!

This phishing simulation was designed to test your online-scam detection skills. Don't worry, your device is safe.

- You've just experienced a simulated phishing attempt as part of our KnowledgeNet interactive scam spotting email course.
- This exercise was designed to help you recognize phishing scams and protect your personal information in the future.
- Had this been an actual phishing attempt, your data could have been compromised. But don't worry—this was just a simulation, and no harm was done.

### What Now?

- Upload a screenshot of this email to our KnowledgeNet forum on moodle, to help others recognize phishing scams like this one. Click the button below to head straight to the KnowledgeNet forum.
- Also, if you have any examples or experiences with online scams you'd like to share, we'd love to hear them! You can contact us directly at [scams@knowledgeflow.org](mailto:scams@knowledgeflow.org)

[KnowledgeNet Forum](#)

# Project KnowledgeLink



## Volunteer with us!

- Help your community stay safe and empowered online
- Receive comprehensive cybersafety training and share your knowledge with others
- Foster a sense of community and belonging while reducing cyber threats

*Funded in part by the 2024-25 Seniors  
Community Grant*

# Project KnowledgeLink: How to Sign Up

- **KnowledgeLink.KnowledgeFlow.org**

## Project KnowledgeLink: Empowering Senior Ambassadors For Digital Safety

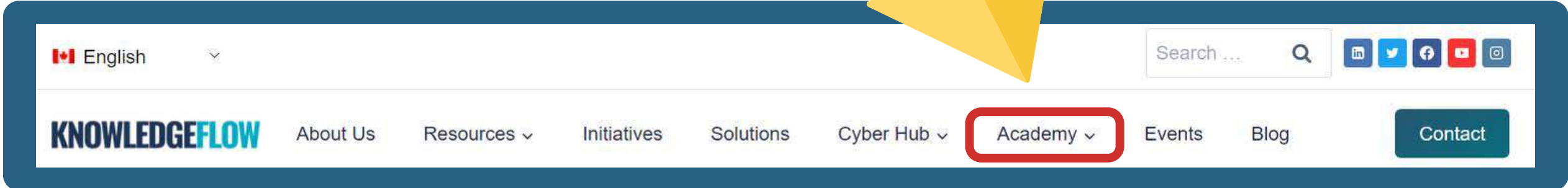
KnowledgeLink, a new initiative by KnowledgeFlow Cybersafety Foundation, aims to protect and empower seniors by enhancing their cybersafety awareness and skills. This community-driven project focuses on training senior ambassadors to serve as local experts in digital safety, helping their peers navigate the online world with confidence.

[Become A Volunteer](#)





# Access Our FREE Courses



**KNOWLEDGEFLOW**  
Cybersafety Academy

Username

Password

[Log in](#)

[Lost password?](#)

**Log in using your account on:**

**Is this your first time here?**  
For full access to this site, you first need to create an account.

[Create new account](#)

English (Canada) (en\_ca)



TheKnowledgeAcademy

# Do you want to make money, fast?

10 Lessons With Guaranteed Results 💰💰💰



- More than \$100K earned
- All free resources
- Learn from the pros!

 1-800-SCAM-101

**ENROLL NOW!**

# Scammer Training 101





1

# Choosing Your Target

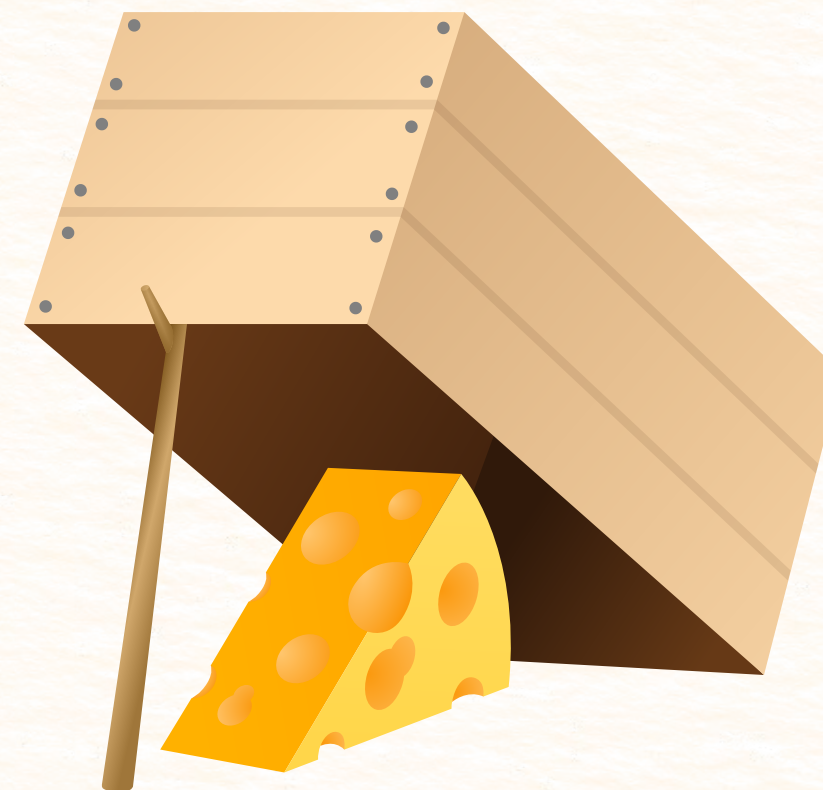
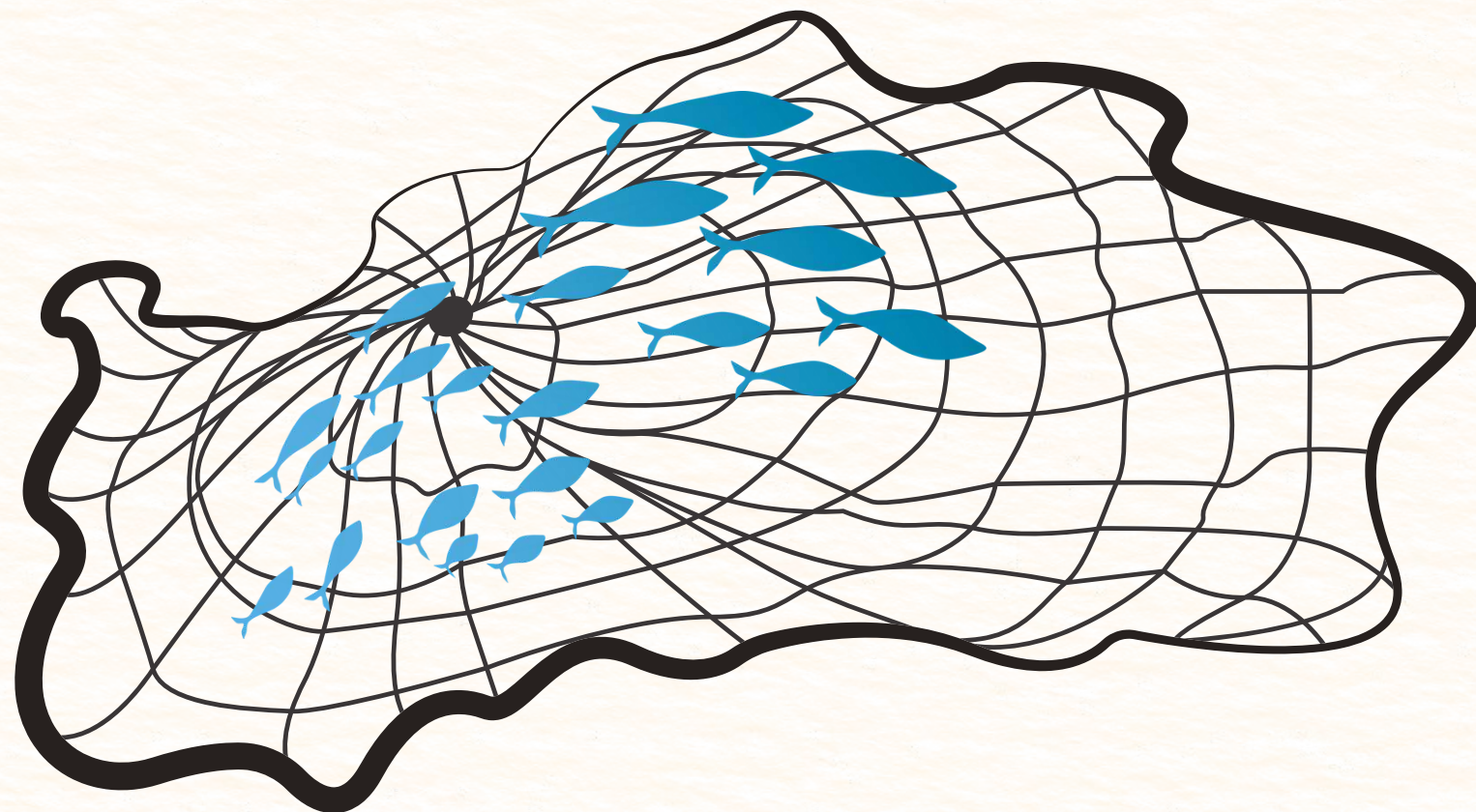
# Scammer Training 101: Choosing Your Target



**Every scammer needs to decide who they're going after.**

Seniors, newcomers, teens, businesses — each target has different weaknesses to exploit.

## Cast a wide net or set a trap?

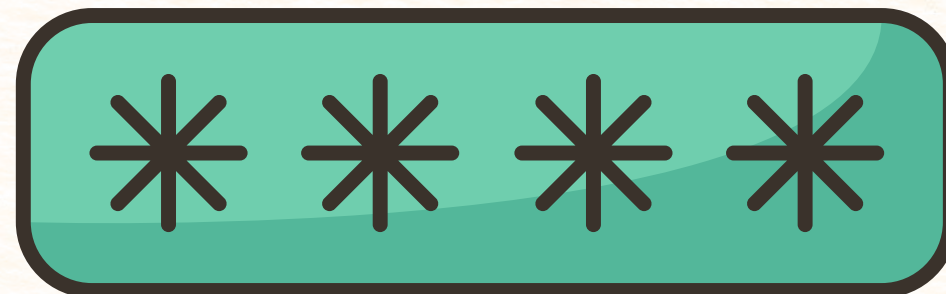


# Scammer Training 101: Choosing Your Target

## What's the Goal?



Scammers may be after money, personal information, or access to personal accounts.





# Choosing Your Vehicle

# Scammer Training 101: Choosing Your Vehicle



**Scammers use different platforms for different roles and targets.**

Each vehicle has its own pros and cons.

## Email



- Allows attachments and links
- Greater length and detail
- Logos and format
- Header spoofing

## Phone



- Caller ID spoofing
- Include additional 'characters'
- Convey emotion
- Customize based on victim's reaction

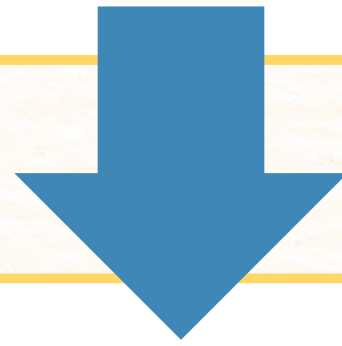
## Text



- Short links and buttons
- Bypass spam filters
- Higher 'open rate'
- Mimic common notifications

# Scammer Training 101: Choosing Your Vehicle

There are many things scammers can do to seem more trustworthy. You can use caller ID spoofing and typosquatting to pose as a legitimate phone number or email.



Scammers will slightly alter phone numbers and emails to look real.

**contact@knowledgeflow.org**



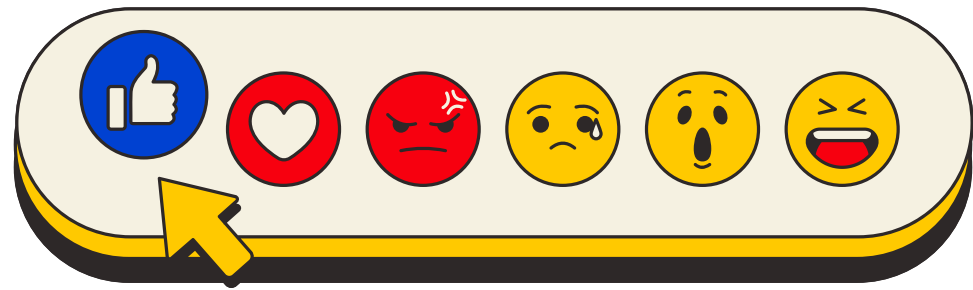
**contactknowledgeflow@email.domain.com**





# Scammer Training 101: Choosing Your Vehicle

## How To Get Your Contact List



**Web scraping** allows scammers to find publicly available personal information like phone numbers and email addresses.



**Security breaches** gather personal information, which is then sold between scammers on the dark web.



Scammers create **ads, newsletters** and **contests** to trick people into entering their contact information.



5

# Crafting the Perfect Story

# Scammer Training 101: Crafting the Perfect Story



**Scammers need a believable story.**

A story helps makes your target want to act, whether the story is urgent, friendly, or official.

## Picking A Role:

To craft your story, scammers should take on roles that seem trustworthy, encouraging their targets to act.

Romantic Interest



Tech Support

Bank Rep



Grandchild

# Scammer Training 101: Crafting the Perfect Story

## Appealing to Emotions:

With these roles, appeal to the targets' emotions through **fear** (ex. a police officer or CRA agent), **excitement** (someone telling you you've won something), or **trust** (ex. family member).

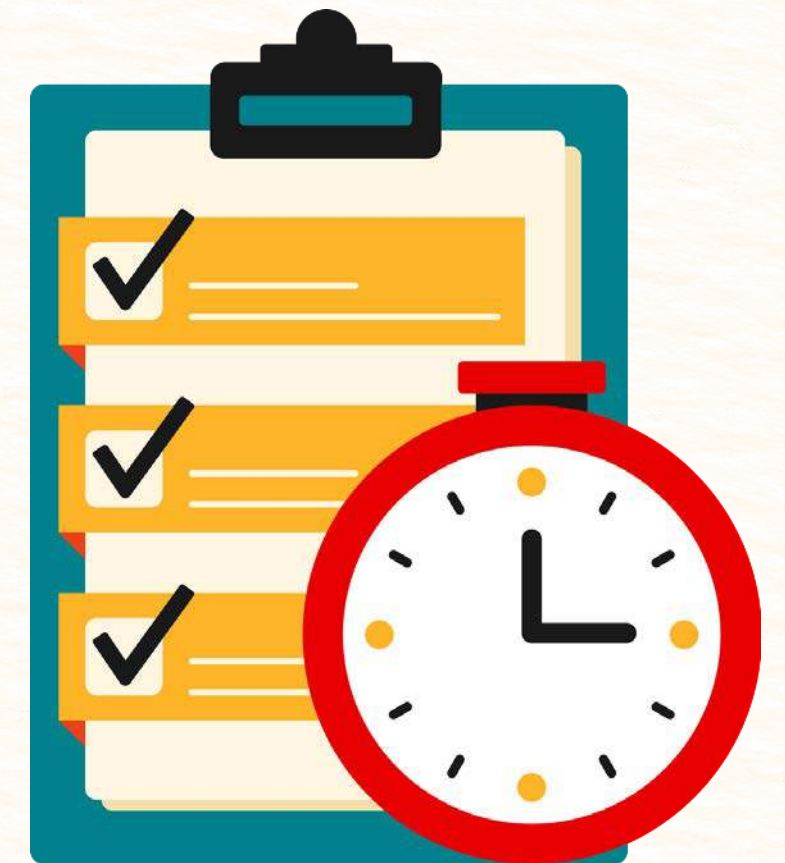


# Scammer Training 101: Crafting the Perfect Story

## Tone and Voice:

### ➤ Urgency and Deadlines

“Act now, or else...” is a scammer’s best friend.



# Scammer Training 101: Crafting the Perfect Story



## Technical Jargon

Overwhelming targets with terms like “account compromise” or “malware infection”



## Fake Contract Details

Using emails or phone numbers that look official.



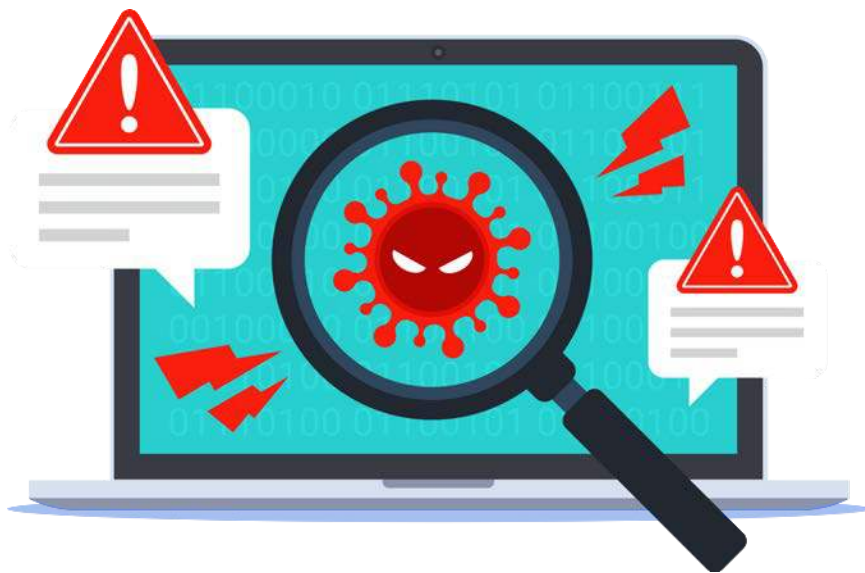


# 4 Choosing Your Tools

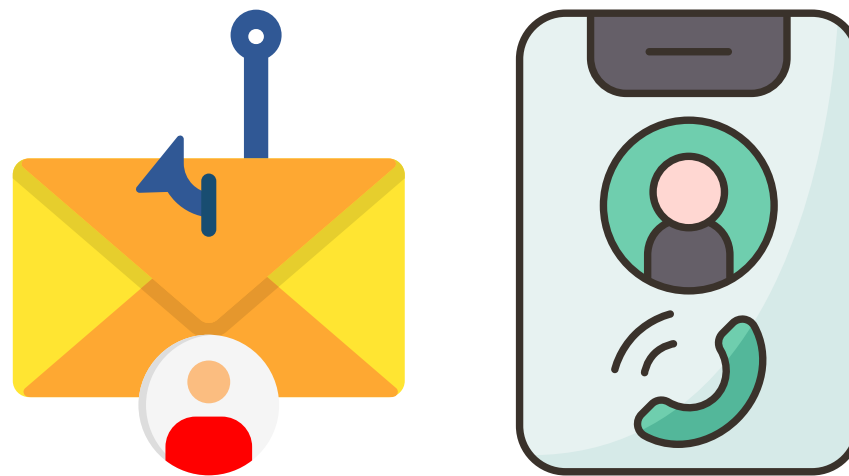
# Scammer Training 101: Choosing Your Tools

 Scammers rely on tools that push people to act quickly and without thinking too much.

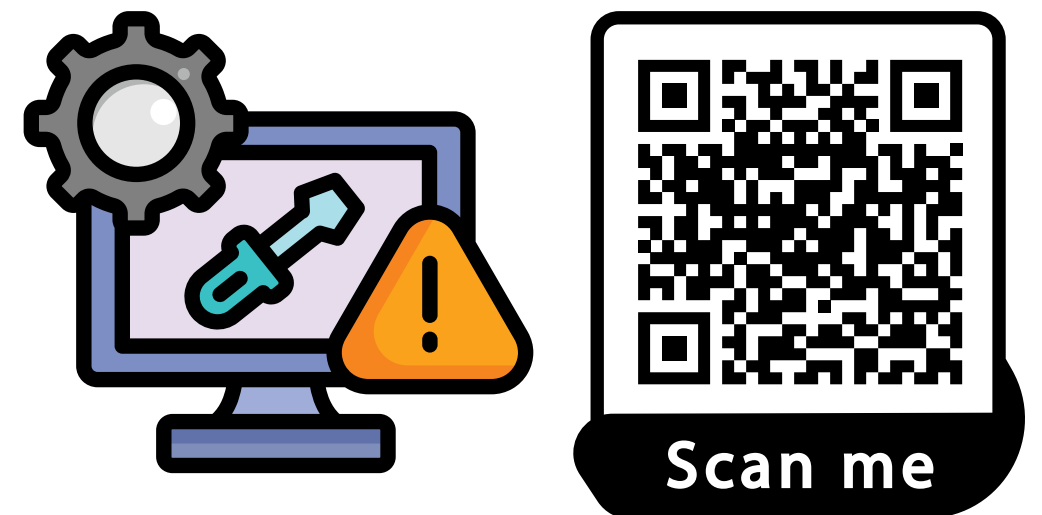
Deliver **malware** to get access to targets' devices and personal information.



Use different types of **spoofing** to fool targets, like Caller ID, SMS, and email domain spoofing.



Make **links** to **fake websites**, use **attachments**, or use **remote access tools**.







5

# Planning the Payoff

How will you get paid?

# Scammer Training 101: Planning the Payoff



Pick payment methods that are quick and hard to trace.

## Gift Cards & Codes

Easy for the target to buy, difficult to trace.

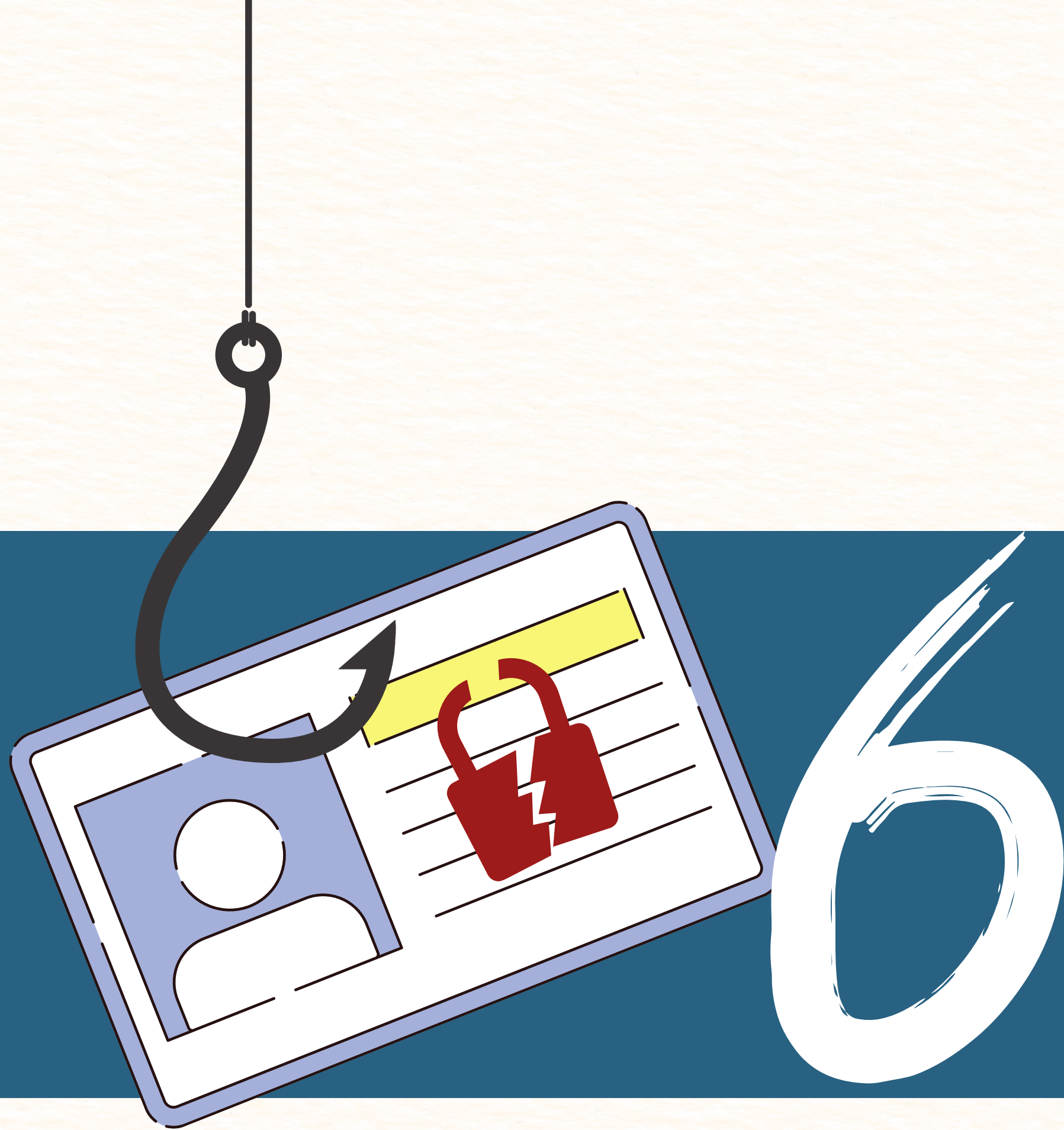


## Wire Transfers

Direct cash, simple to get if the target believes the story.

## Cryptocurrency

Anonymous and now available at local ATM style machines.



# 6 Harvesting Personal Information

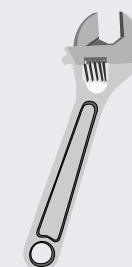
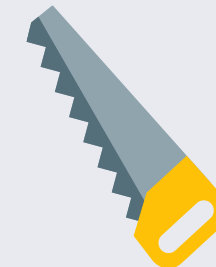
# Scammer Training 101: Harvesting Personal Info



**Not all scammers want money from their targets right away.**

Some scammers are after their targets' personal information to sell or use later. They can use that personal information for identity theft crimes, or piece together information for synthetic identity theft.

## Building a Profile

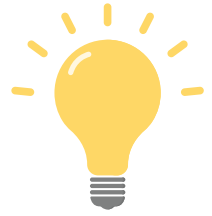


Piece together targets' personal information, such as birthdate, address, and email, to sell or use for identity theft.



# Overcoming Resistance - Handling Doubts

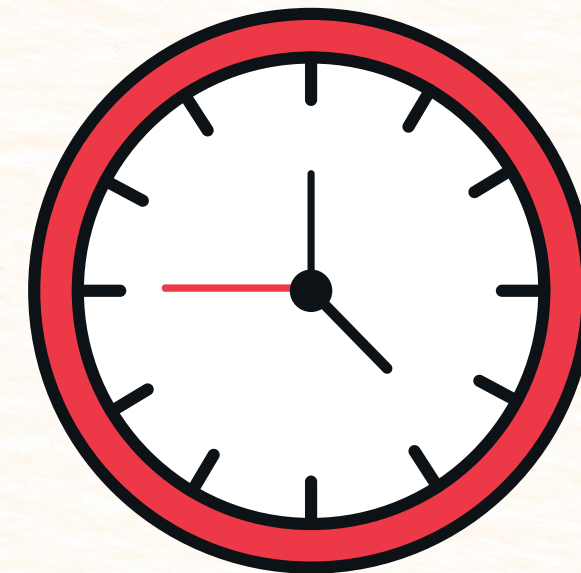
# Scammer Training 101: Overcoming Resistance



Anticipate doubts and be ready with convincing replies.

## Using Pressure Tactics

“If you don’t act, you’ll lose money/time/status.”



# Scammer Training 101: Overcoming Resistance

## Faking Authority

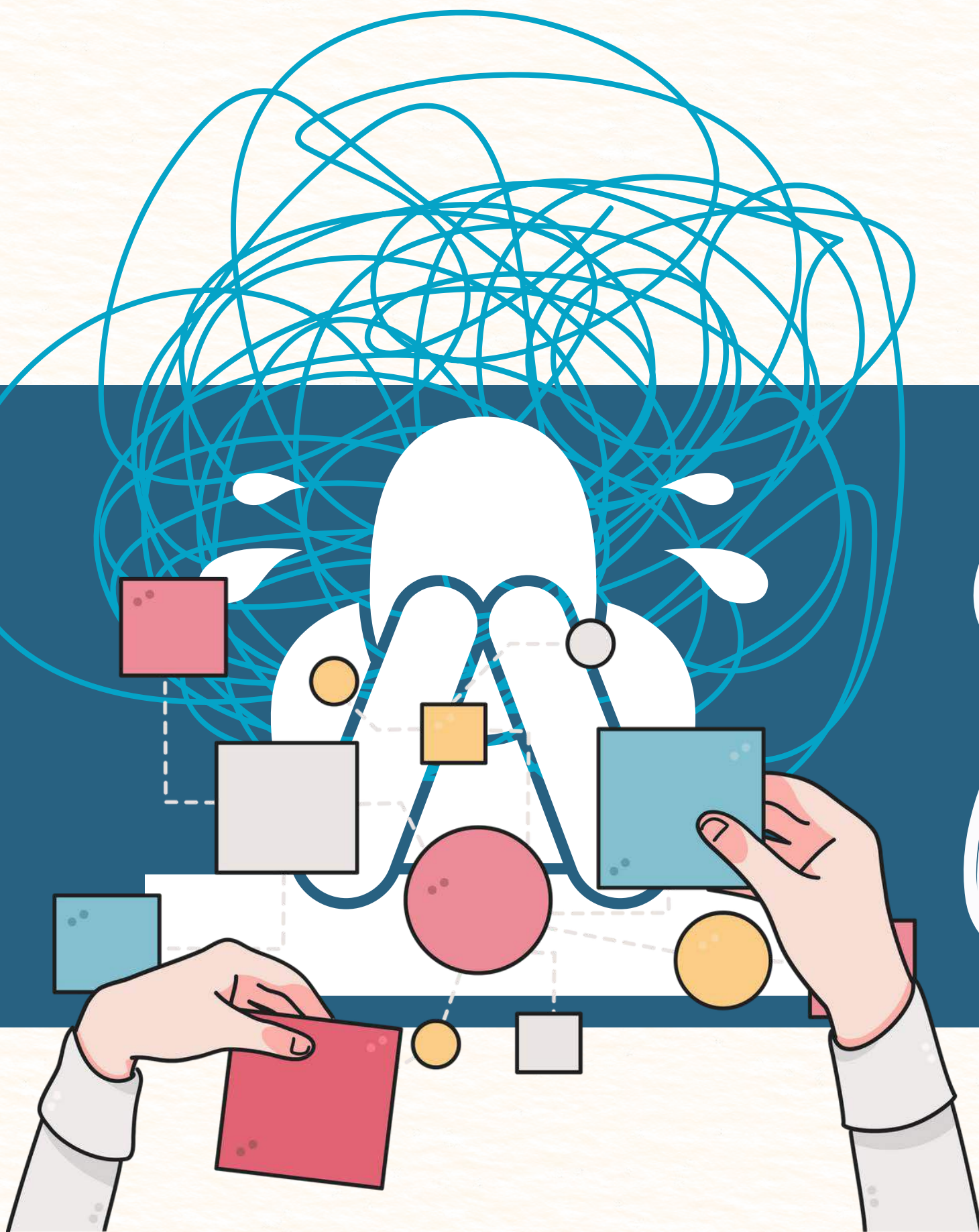
“I’m with [government agency, bank], so you can trust me.”



## Deflecting Questions

Keeping the conversation on the scammer’s terms.





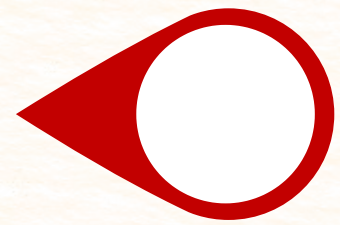
# Running A Long-Term Scam



# Scammer Training 101: Keeping the Victim Engaged

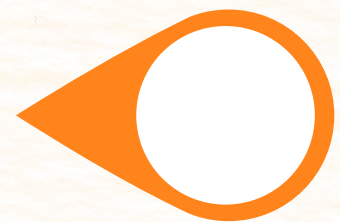


For romance scams or investment schemes, build trust over time.



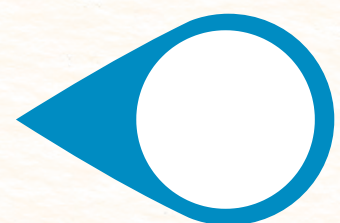
## Appear Consistent and Genuine

Daily conversations, small gifts, or favours.



## Ask for Money Slowly

Start small to build comfort, then increase.



## Use Emotional Manipulation

"I thought we were close. Can't you help me?"





# Scamming in Real Time

Fake Tech Support and Ransomware

# Scammer Training 101: Scamming in Real Time



Pretend to be helpful while you access their device and money.

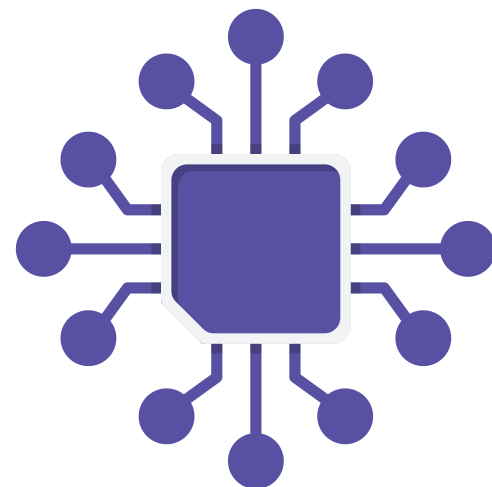
## Phone or Pop-Up Warnings

Posing as support for a “compromised” account or device.



## Remote Access Scams

Convincing targets to install remote software.



## Holding Data for Ransom

Locking the device or data until money is paid.





# Avoiding Detection - Covering Your Tracks

# Scammer Training 101: Avoiding Detection

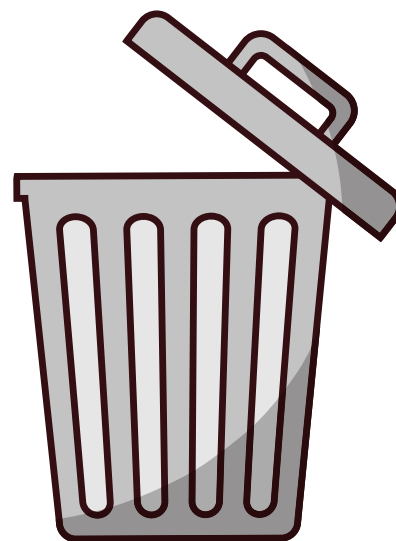


**How to avoid getting caught.**

Use VPN's and proxy servers to hide your location.

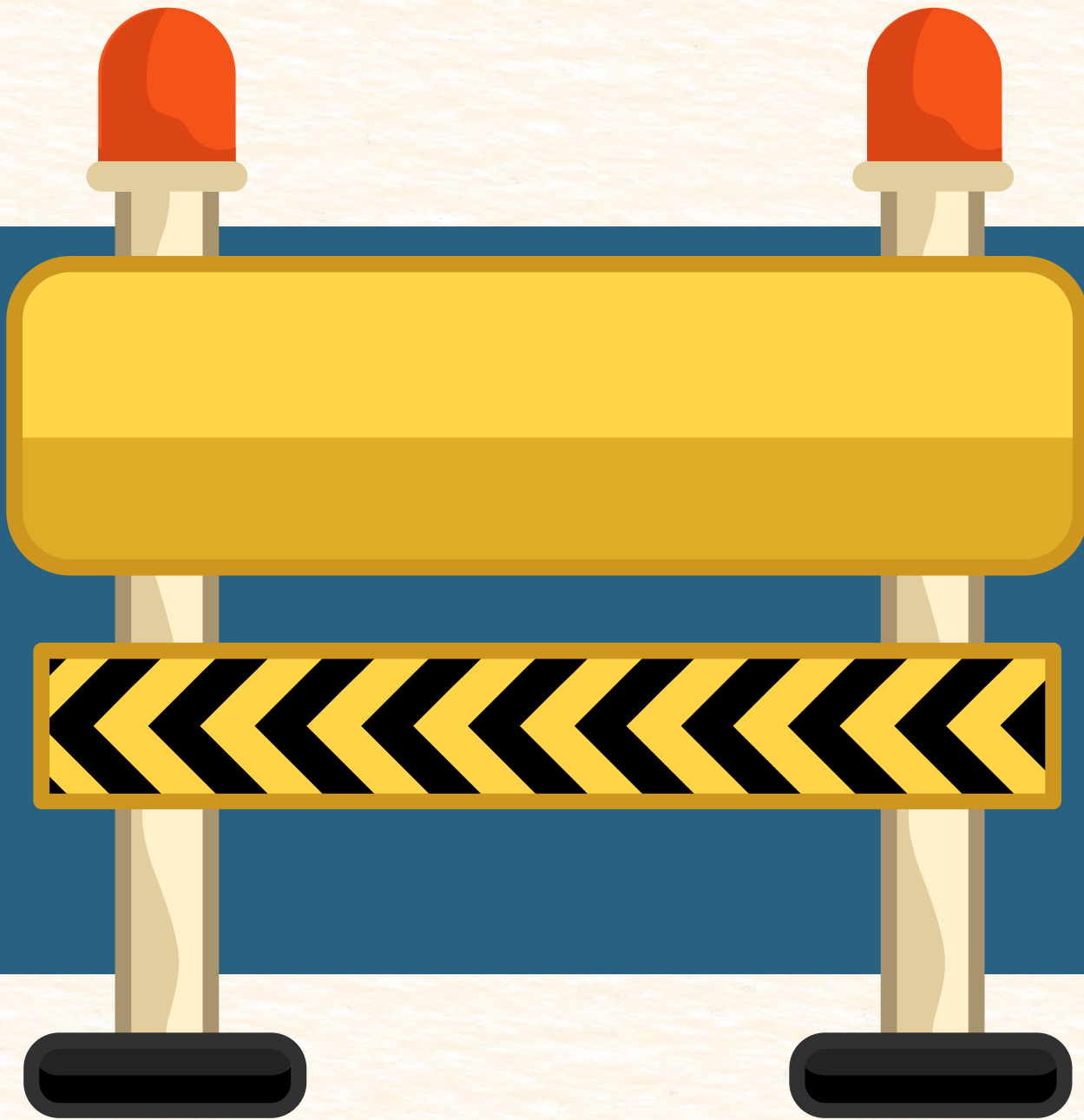


Delete accounts or emails before they can be traced.



Work from jurisdictions that make tracking and coordination difficult for law enforcement.





# Common Roadblocks

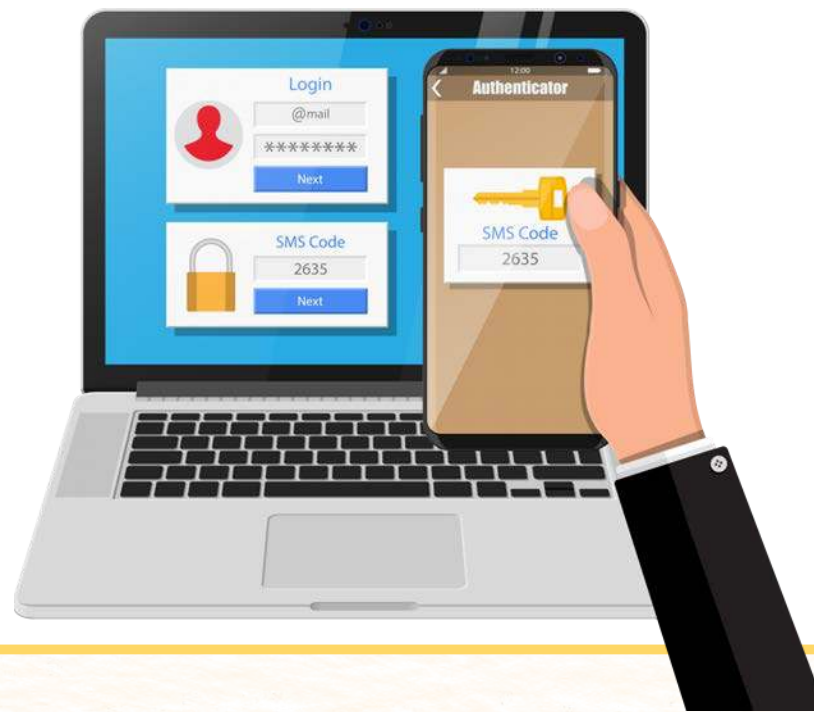
# Scammer Training 101: Common Roadblocks

## Top Reasons Your Scam Might Fail

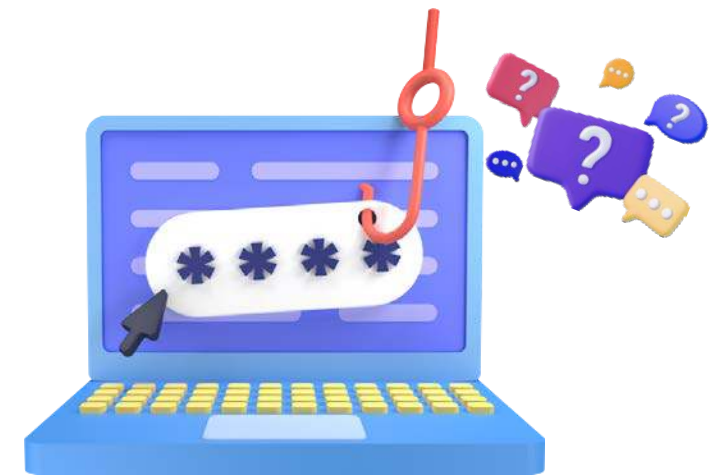
### Passwords that are:

- strong
- long
- unique to each account
- stored securely

### Multi-Factor Authentication



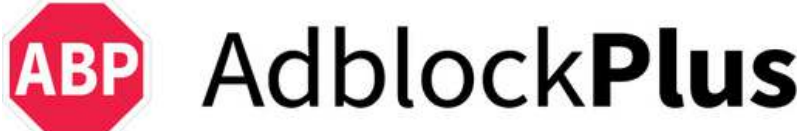
### Password Managers and fake answers to security questions



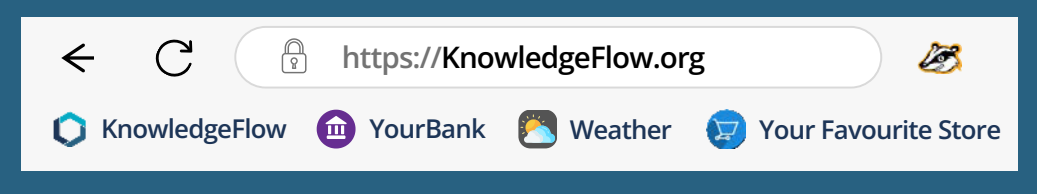
# Scammer Training 101: Common Roadblocks

## Top Reasons Your Scam Might Fail

### Ad Blockers and Privacy Extensions



### Bookmarks instead of searches



### Tiny digital footprints

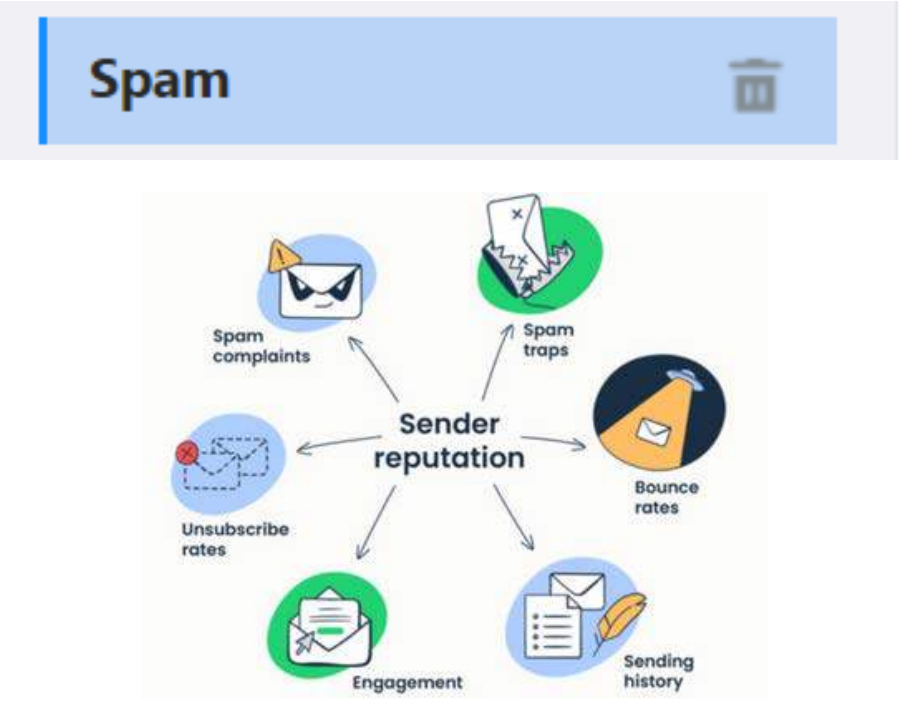




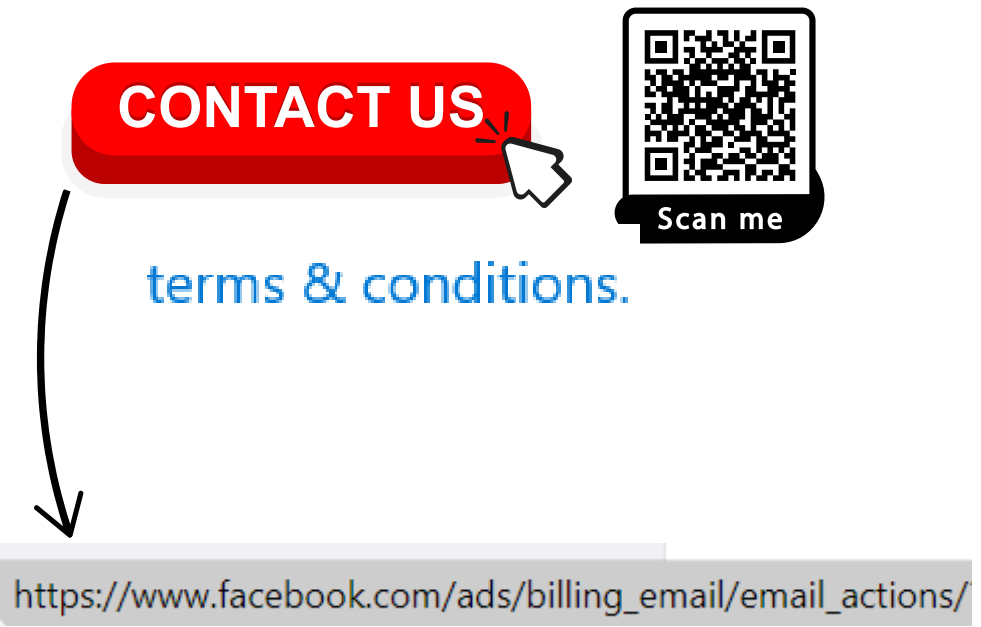
# Scammer Training 101: Common Roadblocks

## Top Reasons Your Scam Might Fail

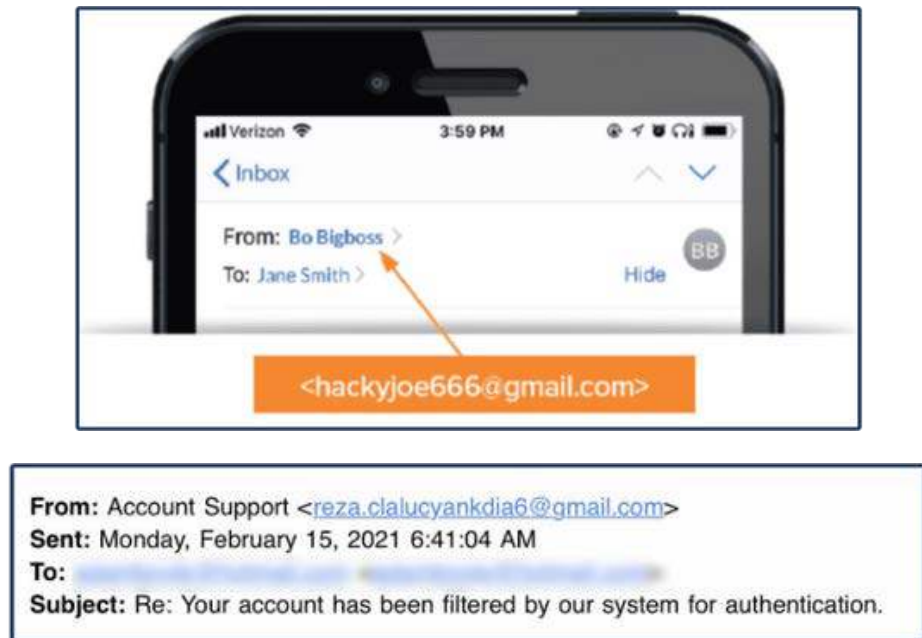
### Spam Filters



### Link Previews



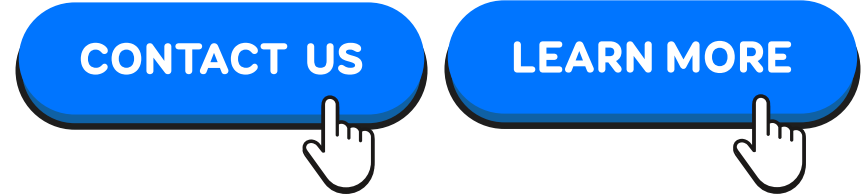
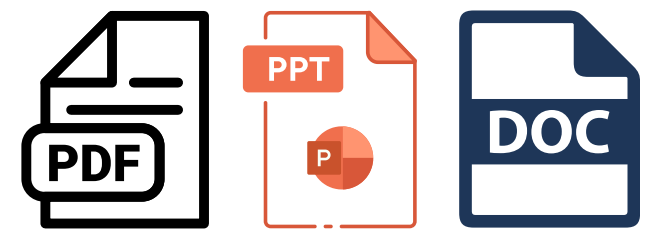
### Email Sender Checks



# Scammer Training 101: Common Roadblocks

## Top Reasons Your Scam Might Fail

People who don't open attachments or click links



People who 'Screen' their calls



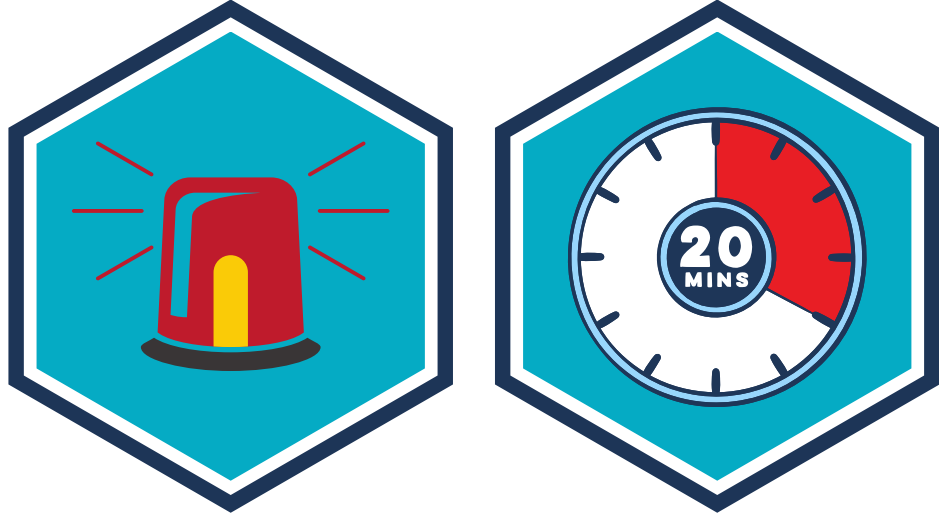
People who aren't afraid to hang-up!



# Scammer Training 101: Common Roadblocks

## Top Reasons Your Scam Might Fail

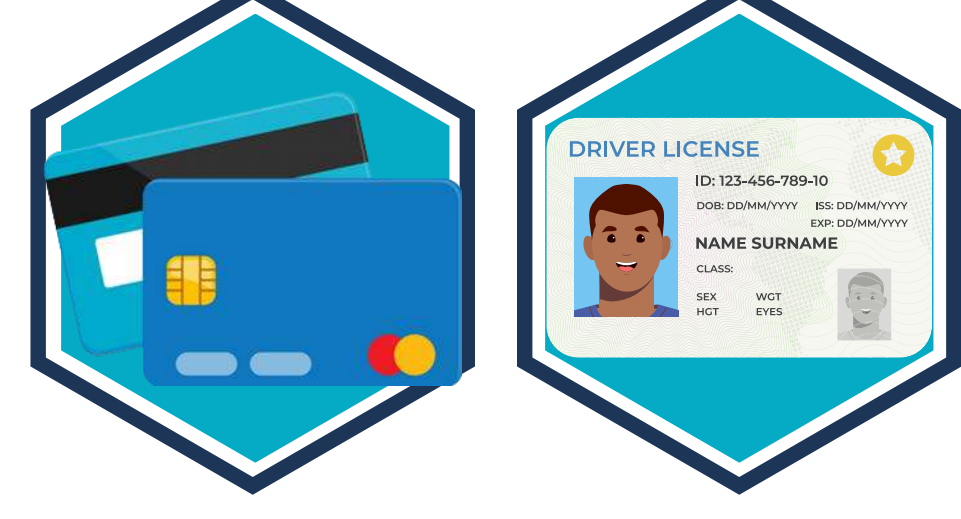
**Skepticism of urgency and deadlines**



**Skepticism of authority and legitimacy**



**Skepticism of requests for payments or info**



# Scammer Training 101: Common Roadblocks

## Top Reasons Your Scam Might Fail

**Someone who thinks like a scammer!**





# How to be #UnHackable

**Be  
Private**

**Be  
Secure**

**Be  
Skeptical**

**Be  
Positive**

## Report Concerns to:

- Canadian Anti-Fraud Centre
- Your bank & Credit Card Company
- Local police department
- Equifax and Transunion for credit alerts
- CRTC - regarding spam emails
- 7726 - forward spam texts
- Federal Privacy Commissioner
- Provincial Privacy Commissioner

**www.KnowledgeFlow.org**  
**CYBER SAFETY TIP SHEET**

**WHAT TO DO AFTER IDENTITY THEFT**

Found out someone's been posting with your social media account?  
Noticed purchases on your credit card bill that you never made?

Other possible signs of Identity Theft:

- Being denied a loan, job or rent unexpectedly
- Bills and statements don't arrive when they are supposed to
- Calls from collection agencies or creditors for an account you don't have

Regardless of how, your data, along with your identity has been stolen, what now?

Suspect a scam? Report fraud:  
[www.antifraudcentre-centreantifraude.ca](http://www.antifraudcentre-centreantifraude.ca)

**1** **Change your passwords.** Never use the same password on more than one account. Enable Two Factor Authentication, and use a password manager to generate and store strong passwords.

**2** **Tell the financial institution, credit card issuers, and companies involved.** You may need to change your account numbers, your PINs, and get new debit and credit cards.

**3** **Report the identity theft to the police and the CAFC.** Get a copy of the police report for your records. Contact the Canadian Anti-Fraud Centre (CAFC) 1-888-495-8501 or visit [www.antifraudcentre-centreantifraude.ca](http://www.antifraudcentre-centreantifraude.ca).

**4** **Cancel any missing or stolen identification documents.** Cancel government-issued documents like driver's license, birth certificate, or health card. Contact Service Ontario at **1-800-267-8097**  
For SIN issues, contact Service Canada: **1-800-622-6232**  
For Passport issues: **1-800-567-6868**

**5** **Contact Equifax and TransUnion.** Request a copy of your credit reports and Dispute the fraudulent debt. Place a "fraud alert" on your file.  
**Equifax 1-800-465-7166**  
[www.equifax.ca](http://www.equifax.ca)  
**TransUnion 1-800-663-9980**  
[www.transunion.ca](http://www.transunion.ca)

**Info@KnowledgeFlow.org**  
**Facebook.KnowledgeFlow.org**  
**LinkedIn.KnowledgeFlow.org**  
**Twitter.KnowledgeFlow.org**

# Stay In Touch!



# Thank You!

info@KnowledgeFlow.org



[www.KnowledgeFlow.org](http://www.KnowledgeFlow.org)



[facebook.KnowledgeFlow.org](https://facebook.KnowledgeFlow.org)



[instagram.KnowledgeFlow.org](https://instagram.KnowledgeFlow.org)



[linkedin.KnowledgeFlow.org](https://linkedin.KnowledgeFlow.org)



[twitter.KnowledgeFlow.org](https://twitter.KnowledgeFlow.org)



[youtube.KnowledgeFlow.org](https://youtube.KnowledgeFlow.org)



# Testing Your Skills

Do you have what it takes?



# Scammer Training 101: Testing Your Skills

## [URGENT] Unauthorized Purchase on Your Account - Action Required

**A** support@kakzjgh881kkzj-billion-alerts.com  
To: you@email.domain

Dear [Name],

We have detected an unusual purchase on your account totalling **\$2,567.89** made on [specific date]. The item in question was purchase from LuxuryTech Online and is scheduled for shipment to an address that does not match your profile.

**If you did not authorize this transaction, please take immediate action to prevent further charges.**

### What to Do Next:

1. Click the link below to access your account and dispute the charges: **[maliciouslink].secure-billing.com/dispute**
2. Open the attached PDF for a detailed invoice of the purchase.

**Attachment: *Invoice\_Transaction\_[random digits].pdf***

Thank you for your prompt attention to this matter.

**Sincerely,**

Fraud Protection Services

*Secure Billing Alerts*

# Scammer Training 101: Testing Your Skills

## [URGENT] Unauthorized Purchase on Your Account - Action Required

**A** support@kakzjgh881kkzj-billion-alerts.com  
To: you@email.domain

Dear [Name],

We have detected an unusual purchase on your account totalling **\$2,567.89** made on [specific date]. The item in question was purchase from LuxuryTech Online and is scheduled for shipment to an address that does not match your profile.

**If you did not authorize this transaction, please take immediate action to prevent further charges.**

### What to Do Next:

1. Click the link below to access your account and dispute the charges: [\[maliciouslink\].secure-billing.com/dispute](#)
2. Open the attached PDF for a detailed invoice of the purchase.

**Attachment: *Invoice\_Transaction\_[random digits].pdf***

Thank you for your prompt attention to this matter.

**Sincerely,**  
Fraud Protection Services  
*Secure Billing Alerts*

How can we  
make this  
better?



# Scammer Training 101: Testing Your Skills

## [URGENT] Unauthorized Purchase on Your Account - Action Required



**support@kakzjgh881kkzj-billion-alerts.com**

To: **you@email.domain**

Dear [Name],

*Make realistic emails so you seem legitimate.*

We have detected an unusual purchase on your account totalling **\$2,567.89** made on [specific date]. The item in question was purchase from LuxuryTech Online and is scheduled for shipment to an address that does not match your profile.

**If you did not authorize this transaction, please take immediate action to prevent further charges.**

### **What to Do Next:**

1. Click the link below to access your account and dispute the charges: **[maliciouslink].secure-billing.com/dispute**
2. Open the attached PDF for a detailed invoice of the purchase.

# Scammer Training 101: Testing Your Skills

## [URGENT] Unauthorized Purchase on Your Account - Action Required

 support@kakzjgh881kkzj-billion-alerts.com  
To: you@email.domain

Dear [Name],

*Good scammers don't make typos or grammar errors.*

We have detected an unusual purchase on your account totalling \$2,567.89 made on [specific date]. The item in question was purchase from LuxuryTech Online and is scheduled for shipment to an address that does not match your profile.

If you did not authorize this transaction, please take immediate action to prevent further charges.

What to Do Next:

# Scammer Training 101: Testing Your Skills

## [URGENT] Unauthorized Purchase on Your Account - Action Required

**A** support@kakzjgh881kkzj-billion-alerts.com  
To: you@email.domain

Dear [Name],

We have detected an unusual purchase on your account totalling **\$2,567.89** made on [specific date]. The item in question was purchase from LuxuryTech Online and is scheduled for shipment to an address that does not match your profile.

**If you did not authorize this transaction, please take immediate action to prevent further charges.**

### What to Do Next:

1. Click the link below to access your account and dispute the charges: [\[maliciouslink\].secure-billing.com/dispute](#)
2. Open the attached PDF for a detailed invoice of the purchase.

**Attachment: Invoice\_Transaction\_[random digits].pdf**

Thank you for your prompt attention to this matter.

Sincerely,  
Fraud Protection Services  
Secure Billing Alerts

*Rename your attachments  
to seem real!*

# Scammer Training 101: Testing Your Skills

## [URGENT] Unauthorized Purchase on Your Account - Action Required

**A** support@kakzjgh881kkzj-billion-alerts.com  
To: you@email.domain

Dear [Name],

We have detected an unusual purchase on your account totalling **\$2,567.89** made on [specific date]. The item in question was purchase from LuxuryTech Online and is scheduled for shipment to an address that does not match your profile.

**If you did not authorize this transaction, please take immediate action to prevent further charges.**

### What to Do Next

1. Click the link below to access your account and dispute the charges: [\[maliciouslink\].secure-billing.com/dispute](#)
2. Open the attached PDF for a detailed invoice of the purchase.

**Attachment: Invoice\_Transaction\_[random digits].pdf**

Thank you for your prompt attention to this matter.

Sincerely,  
Fraud Protection Services  
Secure Billing Alerts

*This is missing a sense of urgency or a deadline to pressure your target into acting fast!*

# Scammer Training 101: Testing Your Skills



## [URGENT] Unauthorized Purchase on Your Account - Action Required

**A** support@secure-billing-alerts.com  
To: you@email.domain

Dear [Name],

We have detected an unusual purchase on your account totaling **\$2,567.89** made on [specific date].

**If you did not authorize this transaction, please take immediate action to dispute this charge.**

### What To Do Next:

1. Click the Contact Us link below to dispute the charges.
2. Open the attached PDF for a detailed invoice of the purchase.

**Attachment: *Invoice\_Transaction.pdf***

Failure to respond within **24 hours** will result in the transaction being nonrefundable. For assistance, please contact our support team immediately by clicking the Contact Us link below.

**Contact Us!**

Thank you for your prompt attention to this matter.

**Sincerely,**  
Fraud Protection Services  
Secure Billing Alerts

*Keep these improvements  
in mind for your next  
scam!*

# Scammer Training 101: Testing Your Skills

## **Phone Call Scam Script**

*Caller tone: Frantic and distressed, with background noise to add to the authenticity.*



# Scammer Training 101: Testing Your Skills

## Phone Call Scam Script

*Caller tone: Frantic and slightly distressed, with background noise to add to the authenticity.*

### **Caller:**

Hi, Grandma/Grandpa? It's me. I'm in trouble, and I don't have much time to talk. I was in an accident, and I need your help right away. I'm okay, but they've taken my phone and wallet. I'm at the police station, but they said I need to pay for damages before I can leave. I'm so embarrassed to ask, but can you send money to cover it?

# Scammer Training 101: Testing Your Skills

## Phone Call Scam Script

*Caller tone: Frantic and slightly distressed, with background noise to add to the authenticity.*

### **Caller:**

Hi, Grandma/Grandpa? It's me. I'm in trouble, and I don't have much time to talk. I was in an accident, and I need your help right away. I'm okay, but they've taken my phone and wallet. I'm at the police station, but they said I need to pay for damages before I can leave. I'm so embarrassed to ask, but can you send money to cover it?

1

***Pause for grandparent's response.***

*Caller tone: Increased urgency.*

2

# Scammer Training 101: Testing Your Skills

## Phone Call Scam Script

*Caller tone: Frantic and slightly distressed, with background noise to add to the authenticity.*

### **Caller:**

Hi, Grandma/Grandpa? It's me. I'm in trouble, and I don't have much time to talk. I was in an accident, and I need your help right away. I'm okay, but they've taken my phone and wallet. I'm at the police station, but they said I need to pay for damages before I can leave. I'm so embarrassed to ask, but can you send money to cover it?

1

***Pause for grandparent's response.***

*Caller tone: Increased urgency.*

### **Caller:**

Please, can you send an eTransfer to the police station so they can process this right now? It's the only way I can get out. They said if you don't pay within the next hour, I will have to stay in jail overnight. Please don't tell Mom or Dad—I'll explain everything when I'm out. I just need your help.

2

# Scammer Training 101: Testing Your Skills

**Instructions if the grandparent agrees:**

**Caller:**

The email for the eTransfer is [fake email]. Send it right now. Thank you so much. I don't know what I'd do without you.

# Scammer Training 101: Testing Your Skills

*Instructions if the grandparent agrees:*

**Caller:**

The email for the eTransfer is [fake email]. Send it right now. Thank you so much. I don't know what I'd do without you.

**B-**

Good start! See feedback attached for improvements

**How can we improve this?**

# Scammer Training 101: Testing Your Skills

*Instructions if the grandparent agrees:*

**Caller:**

The email for the eTransfer is [fake email]. Send it right now. Thank you so much. I don't know what I'd do without you.

**B-**

Good start! See feedback attached for improvements

3

**How can we improve this?**

## **Caller ID Spoofing**

Caller ID spoofing is a tool that causes the caller ID to display a fake phone number, helping fool your target.

Use the real number of the local police department!

# Scammer Training 101: Testing Your Skills

**Instructions if the grandparent agrees:**

**Caller:**

The email for the eTransfer is [fake email]. Send it right now. Thank you so much. I don't know what I'd do without you.

**B<sup>-</sup>**

Good start! See feedback attached for improvements

3

**How can we improve this?**

**Know Your Role**

Spend some time researching your victim on social media to help you be more believable.

Implement these changes next time for an A+!

# Scammer Training 101: Testing Your Skills

**Instructions if the grandparent agrees:**

**Caller:**

The email for the eTransfer is [fake email]. Send it right now. Thank you so much. I don't know what I'd do without you.

**B-**

Good start! See feedback attached for improvements

3

**How can we improve this?**

**Caller ID Spoofing**

Caller ID spoofing is an attack that causes the caller ID to display a fake phone number, helping fool your target.

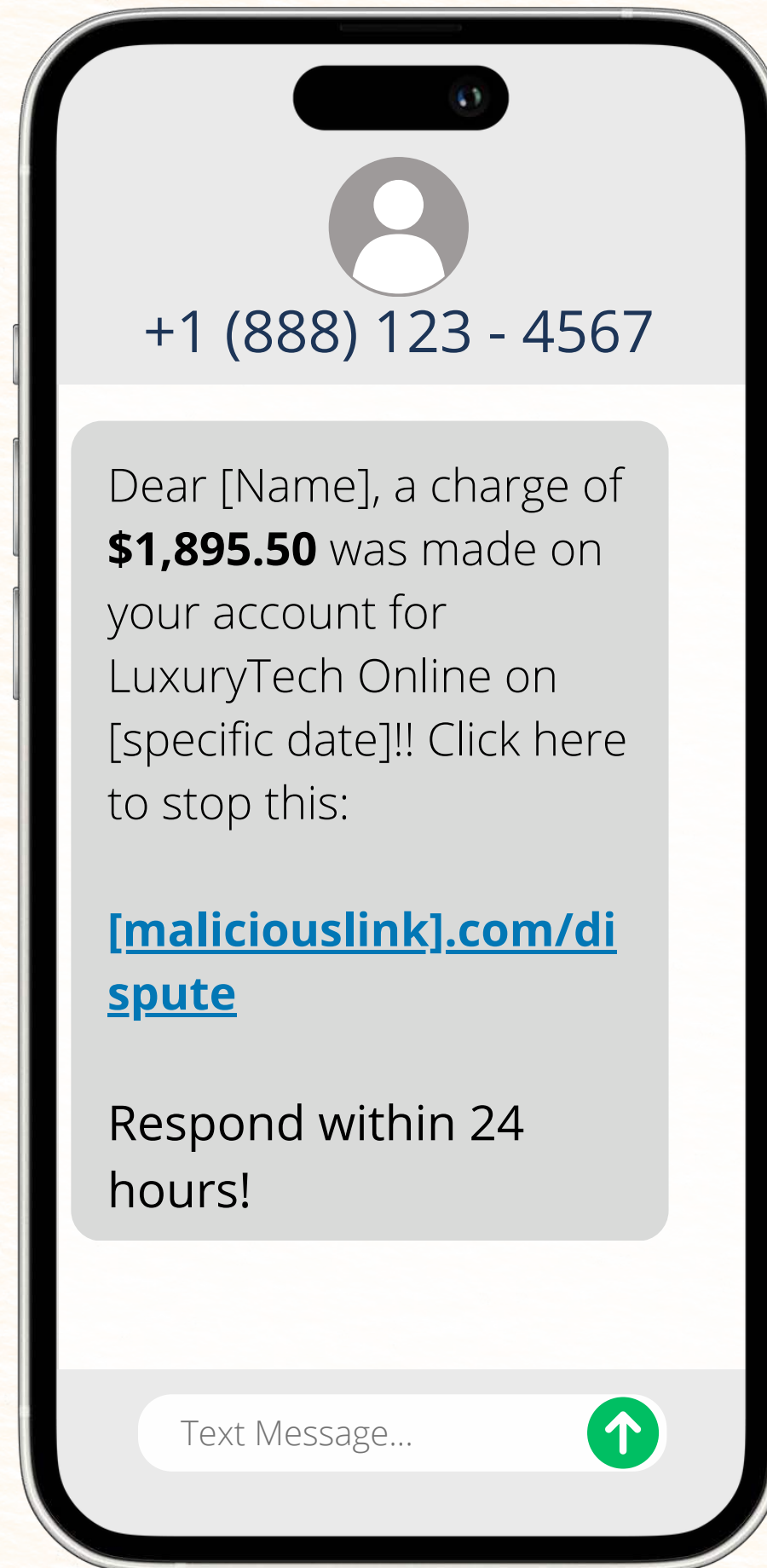
**Know Your Role**

Spending time researching your victim on social media can help you be more believable.

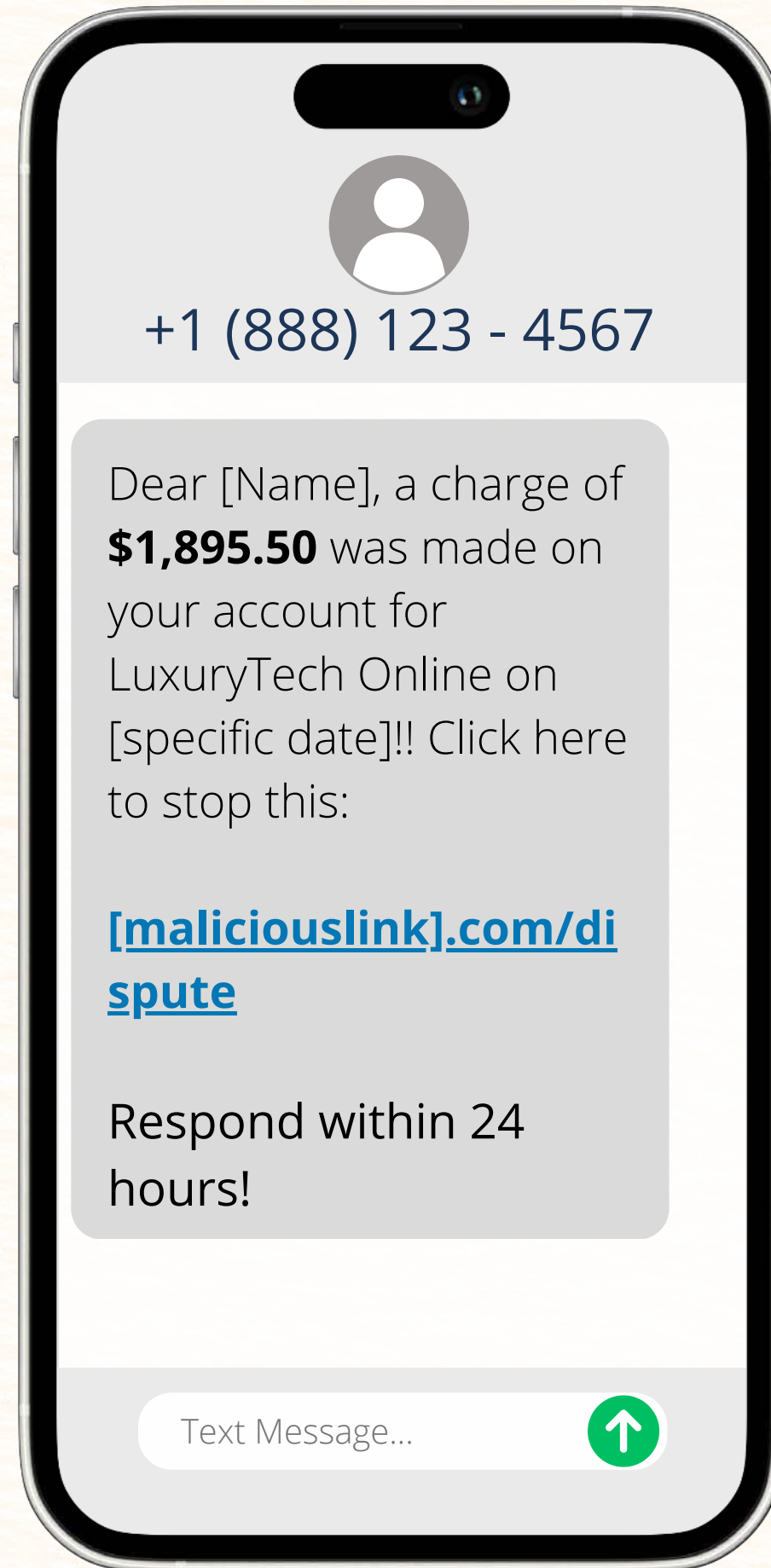
Implement these changes next time for an A+!



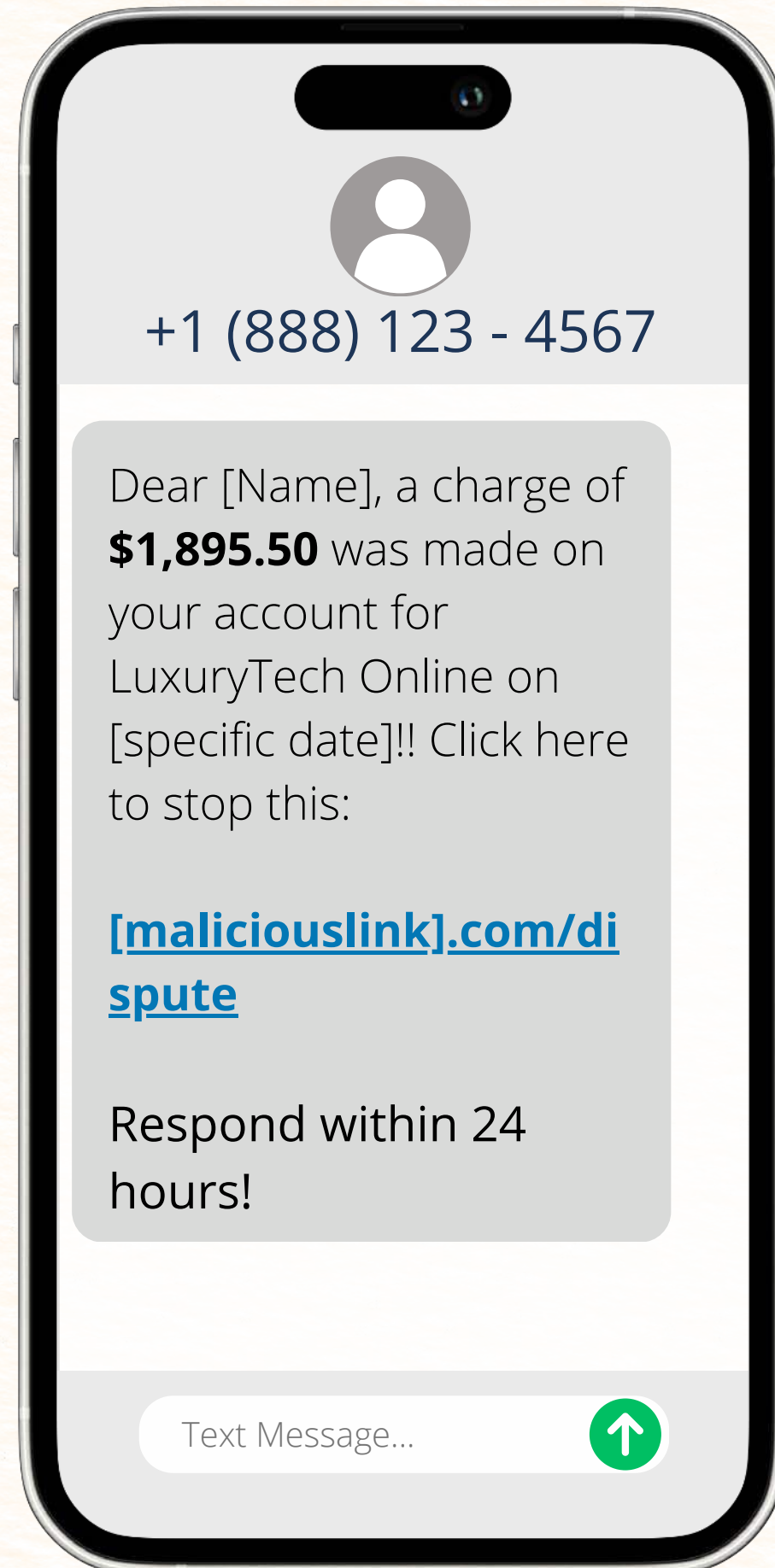
# Scammer Training 101: Testing Your Skills



# Scammer Training 101: Testing Your Skills



# Scammer Training 101: Testing Your Skills



*Let's make a few improvements!*

# Scammer Training 101: Testing Your Skills

*SMS Spoofing  
immediately  
increases your  
credibility!*

A smartphone screen is shown, displaying a text message. At the top, there is a grey header with a white person icon and the text 'LuxuryTech Support' in blue, which is enclosed in a red rectangular box. Below this, the message content is displayed in a grey box. It starts with a red star icon followed by the text 'Alert: Unauthorized Purchase Detected'. The message continues with 'Dear [Name], a charge of \$1,895.50 was made on your account for LuxuryTech Online on'.

 **Alert: Unauthorized Purchase Detected**

Dear [Name], a charge of  
**\$1,895.50** was made on  
your account for  
LuxuryTech Online on

# Scammer Training 101: Testing Your Skills

*An  
explanation  
with context  
helps your  
target believe  
you!*

## **Alert: Unauthorized Purchase Detected**

Dear [Name], a charge of **\$1,895.50** was made on your account for LuxuryTech Online on [specific date]. If you did NOT authorize this transaction, you must take action immediately to prevent further processing.

# Scammer Training 101: Testing Your Skills

**charge:** 📌

[\[maliciouslink\].com/dispute](#)

Failure to respond within 24 hours may result in the charge being processed. For more details, please view your invoice in the secure PDF linked above.

**Support Team**

*Good use of creating a sense of urgency and maintaining professional language*

# Scammer Training 101: Testing Your Skills

**charge:** 📌

[\[maliciouslink\].com/dispute](#)

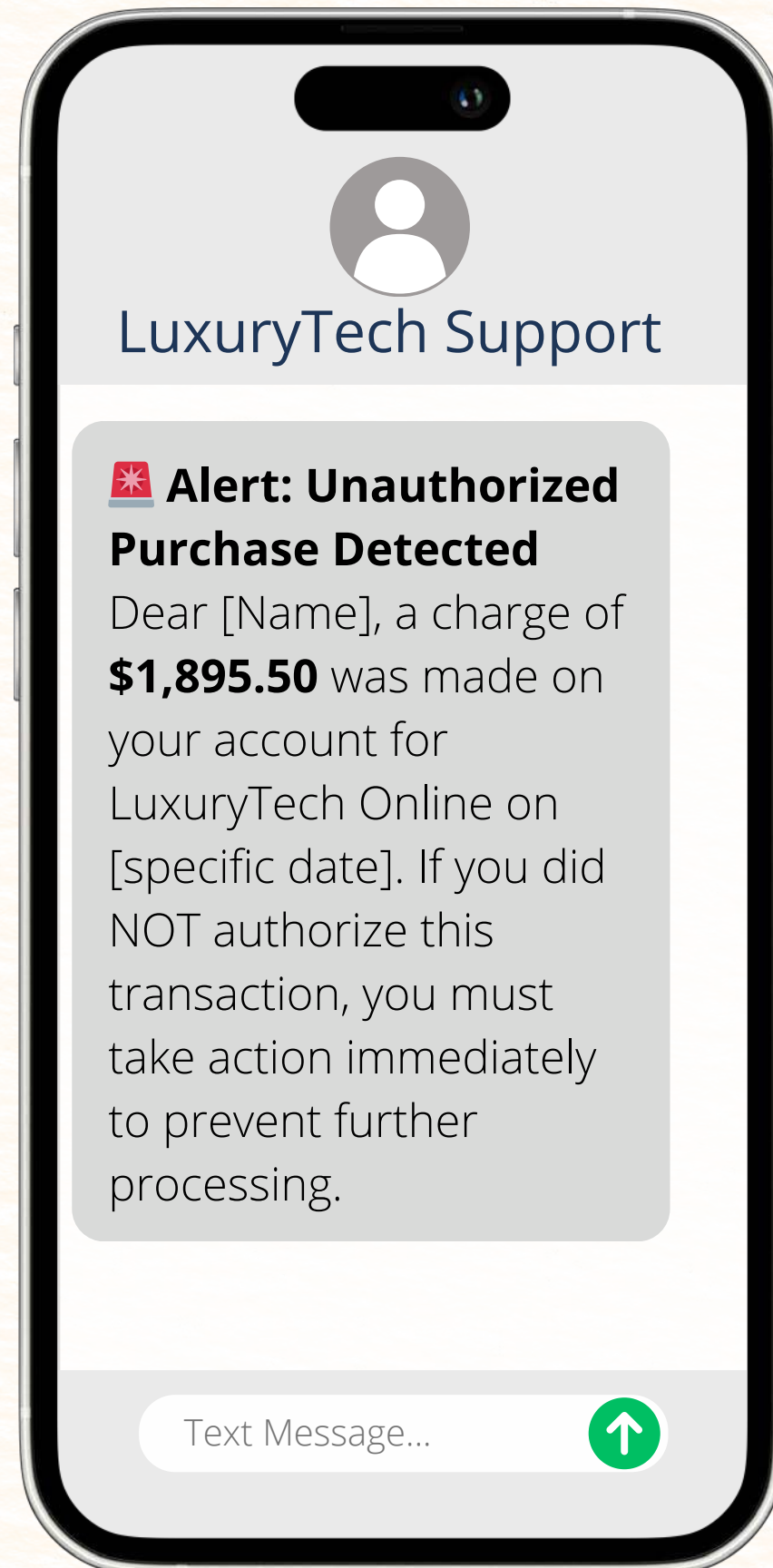
Failure to respond within 24 hours may result in the charge being processed. For more details, please view your invoice in the secure PDF linked above

**Support Team**

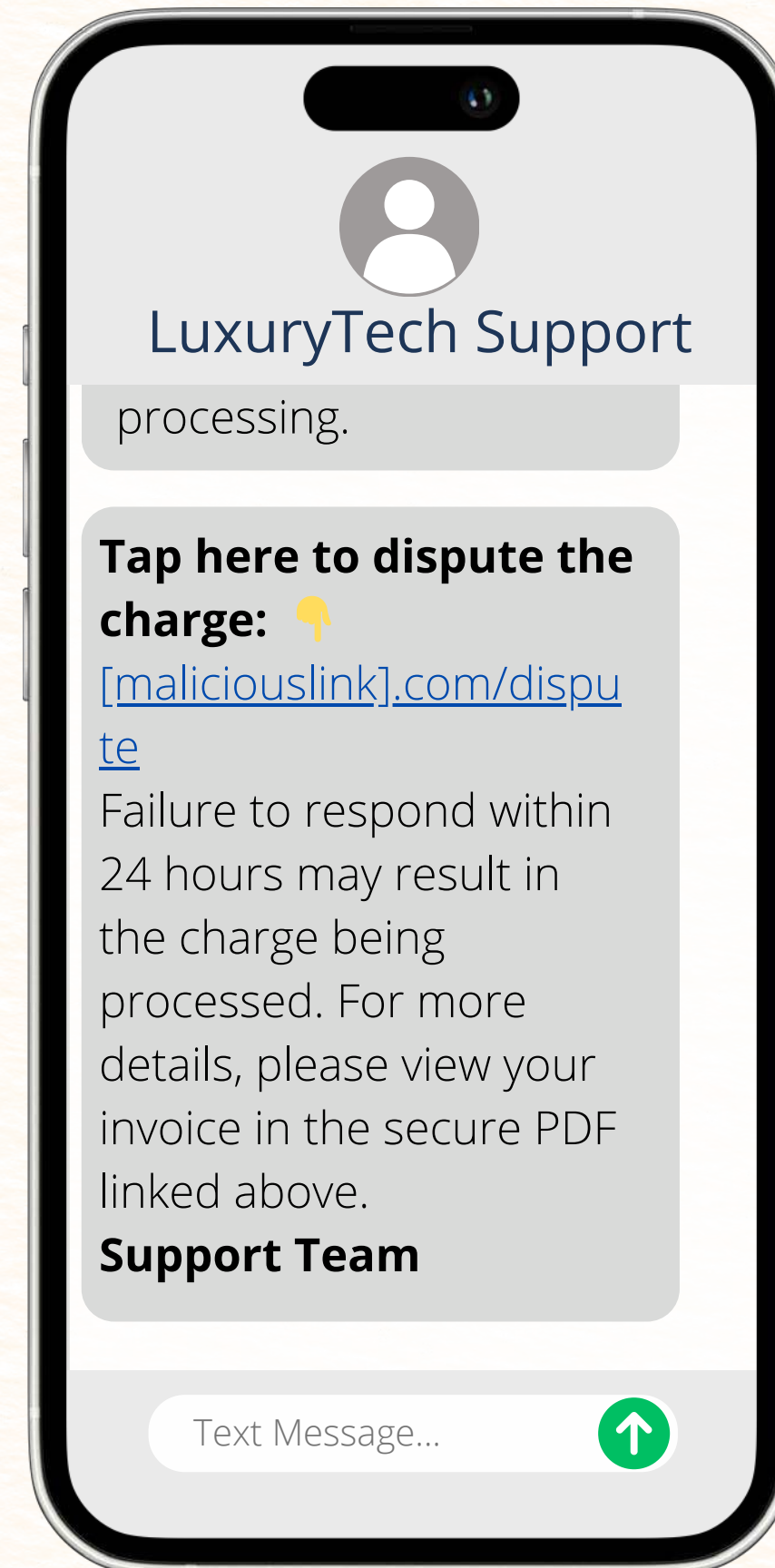
*A trustworthy sign off - good detail!*

# Scammer Training 101: Testing Your Skills

*SMS Spoofing immediately increases your credibility!*



*An explanation with context helps your target believe you!*



**A+**

*Good use of creating a sense of urgency and maintaining professional language*

*A trustworthy sign off - good detail!*



# Stay In Touch!



# Thank You!

info@KnowledgeFlow.org



[www.KnowledgeFlow.org](http://www.KnowledgeFlow.org)



[facebook.KnowledgeFlow.org](https://facebook.KnowledgeFlow.org)



[instagram.KnowledgeFlow.org](https://instagram.KnowledgeFlow.org)



[linkedin.KnowledgeFlow.org](https://linkedin.KnowledgeFlow.org)



[twitter.KnowledgeFlow.org](https://twitter.KnowledgeFlow.org)



[youtube.KnowledgeFlow.org](https://youtube.KnowledgeFlow.org)