Guide to Identifying and Handling Text or Impersonation Scams

1. What Is a Text or Impersonation Scam?

These scams involve messages, often via SMS, email, or messaging apps, where attackers pretend

2. Common Signs of a Scam

Message Red Flags to Watch

For:

- Urgency or pressure: 'Act now or lose access!'
- Unusual requests: Asking for gift cards, wire transfers, or login credentials.
- Spoofed identities: Appears to be from a known contact but uses a different number or email.
- Poor grammar or formatting: Typos, strange phrasing, or inconsistent branding.
- Suspicious links: URLs that don't match the official domain.

3. How to Handle a Suspected Scam Message

Do This:

- Verify the sender using known contact info.
- Report the message to your phone provider, IT team, or FTC.
- Block Phone Number.
- Delete the message.
- Enable spam filters.

Don't Do This:

- Don't click suspicious links.
- Don't reply.
- Don't share personal or financial information.

4. Tips to Stay Safe

- Use multi-factor authentication (MFA).
- Keep software updated.
- Educate your team.
- Use a password manager or vault

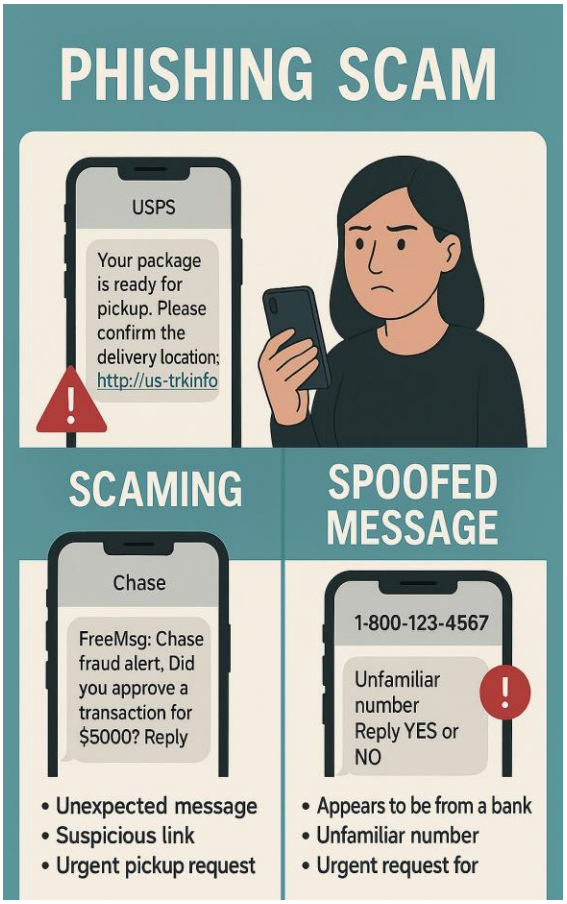
5. Quick Reference Checklist

Red Flag	**Description**
Urgency	'Act now!' or 'Immediate action required'
Unknown Sender	Number/email doesn't match known contact
Suspicious Link	URL looks odd or doesn't match official domain
Request for Money	Gift cards, wire transfers, crypto
Poor Grammar	Typos, strange phrasing, inconsistent tone

847-888-1900
2494 Technology Dr,
Elgin, Illinois 60124
support@
ctinc.com

CTI TECHNOLOGY
we make IT happen

MacHero™



How to Identify and Handle TEXT OR IMPERSONATION SCAMS

These scms Involve messages—often via SMS, email, or mesaging.apps—where attackers pretend to be scmeone trustworthy (e.g. a boss, bank, government agency) to trick you into giving up money.

1 WHAT IS A TEXT OR IMPERSONATIAN SCAM?

Red flags to watch For:

- **Urgency** or pressure: Act now!' or lose access/" ⌞⊐
- **Unusual request:** Asking for gift cards, wire transfers, or login credentials
- **Spooted identities:** Appears to be from a known contact but uses a different number or email
- **Poor grammar or formatting:** Typo, strange phrasing, inconsistent brandi
- **Suspicious links:** URLs that don't match the official domain

VISUAL EXAMPLES OF SCAM MESSAGES

4 HOW TO HANDLE A SUSPECTED SCAM MESSAGE

'Do This:	Don't Do This
Verify the sender contact the per-son or organizau directly using known contact info	Don't click suspicious links
Report the mes-sage.	Don't reply, even to say' Stop
	Don't share personp't ot 'tinancial information

- **Verify the sender** Contact the person or organizabus diree, ly'using known con.
- **Report the me ssage**
  - on your shonk" Black à Report-opt
  - to your IT security tsare.It it's work related
- To FTC ReportFra gov
- **Don't click suspicious links**
- **Don't reply. even te say Stop**
- **Don't share** personal or **financial** information

5 TIPS TO STAY SAFE

- ✓ Use muiti-factor authentication (MFA)
- ✓ Keep software updated to patch security vulnerabilities
- ✓ Educate your team: Regular training on phishing and impersonation tactics
- ✓ Use a password manager

6 QUICK REFERENCE CHECKLIST

Red Flag	Description
✓ Urgency	'Act nowin' or Immediate action required
✓ Unknow Sender	Number donal deam't materan contact
✓ Suspicious Link	URL ooks odd or dotan'leauth cfitcal deprain
✓ Request for Money	Gifficards, wire transters.

847-888-1900

2494 Technology Dr,
Elgin, Illinois 60124

support@
ctinc.com