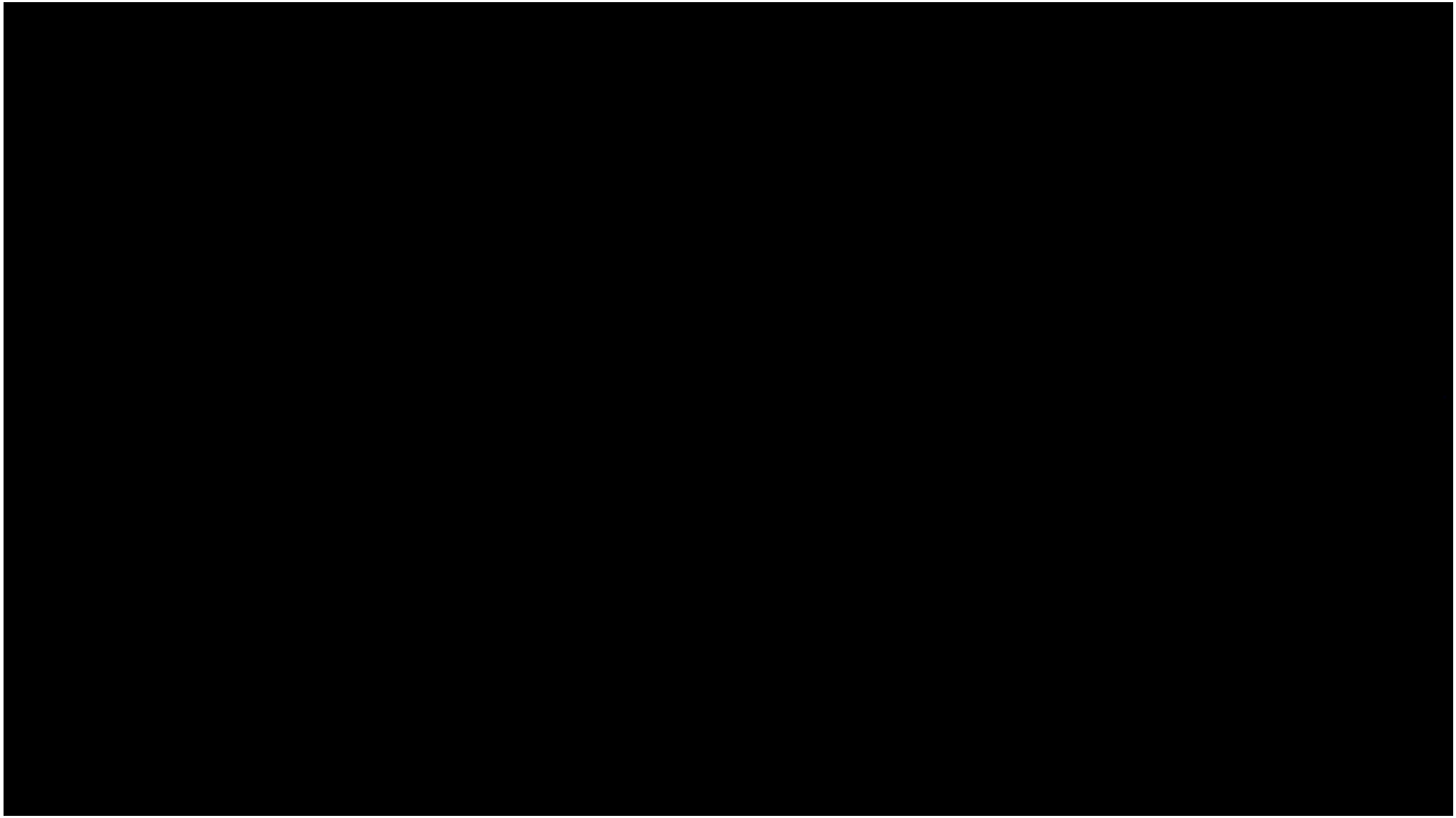
Phishing

Fishing or Phishing?



Definition

- Phishing: an attempt to trick victims into sharing sensitive information such as passwords, usernames, and credit card details for malicious reasons.
- Phishing can be in the form of emails, social media messages, texts, or phone calls.
- General phishing attempts are sent to a large amount of people at the same time with the hope that someone will click on on a link and provide their personal information.

Definition

- Spear-phishing: An attempt to trick a specific victim into sharing sensitive information.
- Often appear to be from a legitimate sender or someone familiar to the victim
- Messages are modified to specifically address a victim
- Includes personal information about the victim, usually obtained from social media

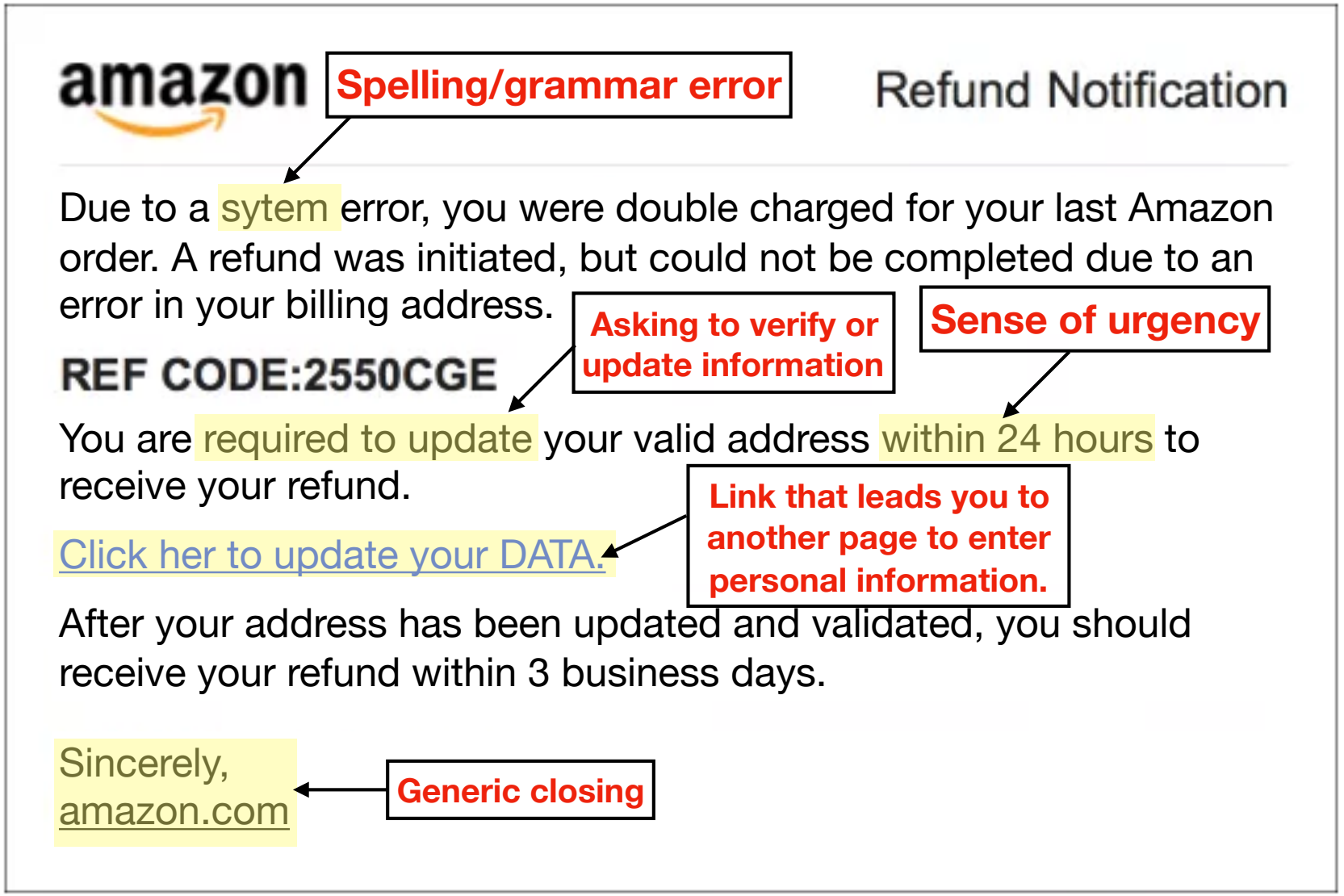
Features of a Phishing Attack

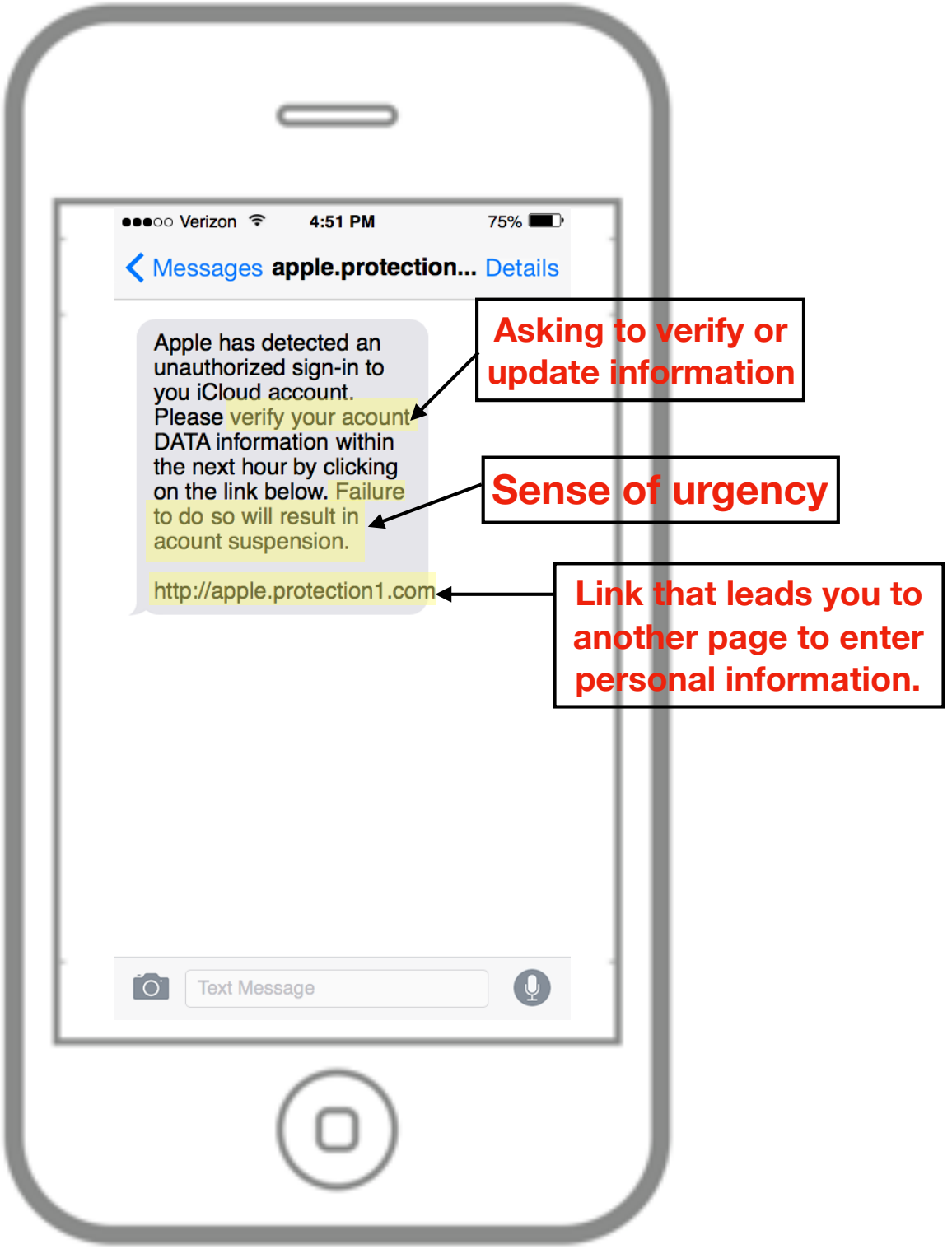
- Asks you to verify or update account information, such as name, date of birth, mothers maiden name, security questions, credit card information, and password.
- The tone gives a sense of urgency or that you're in trouble. You have a limited time to respond.
- There are spelling and grammar errors.

Features of a Phishing Attack

- What they're saying sounds too good to be true.
- The greeting or closing is generic. The greeting might say "Dear Valued Customer"
- Links or attachments that lead you to a login page or a online form where you will have to provide personal information.

Examples of Phishing Attacks


amazon
Spelling/grammar error
Refund Notification
Due to a sytem error, you were double charged for your last Amazon order. A refund was initiated, but could not be completed due to an error in your billing address.
Asking to verify or update information
Sense of urgency
REF CODE:2550CGE
You are required to update your valid address within 24 hours to receive your refund.
Link that leads you to another page to enter personal information.
Click her to update your DATA.
After your address has been updated and validated, you should receive your refund within 3 business days.
Sincerely,
amazon.com
Generic closing


●●●○○ Verizon
4:51 PM
75%
Messages apple.protection... Details
Apple has detected an unauthorized sign-in to you iCloud account. Please verify your acount DATA information within the next hour by clicking on the link below. Failure to do so will result in acount suspension.
http://apple.protection1.com
Text Message
Asking to verify or update information
Sense of urgency
Link that leads you to another page to enter personal information.

Dear Gmail User,

Generic greeting

Spelling/grammar error

As part of our security measures, we regularly update all acounts on our database system. We are unable to update your email account and therefore will be cooling your email account to enable the web upgrade.

You have been sent this invitation because our records indicate you are currently a user whose account has not been activated. We are therefore sending you this email so that you can inform us whether you still want to use this account. If you are still interested in having this accou please update your DATA immediately because out system requires an account verificatio update.

DATA

Asking to verify or update information

To prevent an interruption with your Gmail services, please take a few moments to update your account by filling out the verification and update form immediately.

Click here to verify your account.

Link that leads you to another page to enter personal information.

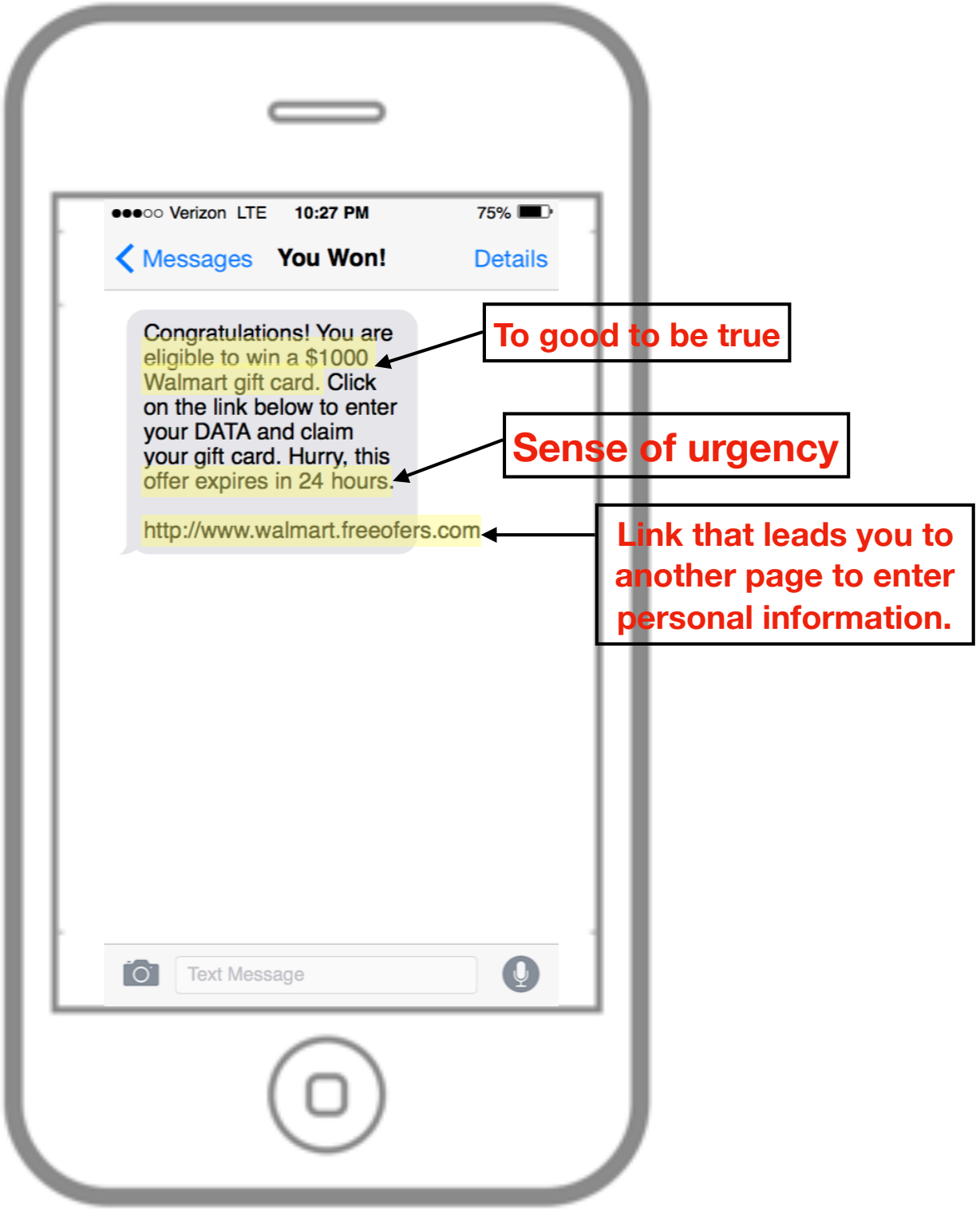
Warning! Any account owner that refuses to update their account after receiving this email will lose their account permanently.

Sense of urgency

We appreciate your cooperation in this matter.

Sincerely,
Gmail Member Services Team

Generic closing


●●●○○ Verizon LTE 10:27 PM 75%
Messages
You Won!
Details
Congratulations! You are eligible to win a $1000 Walmart gift card. Click on the link below to enter your DATA and claim your gift card. Hurry, this offer expires in 24 hours.
http://www.walmart.freeofers.com
Text Message
To good to be true
Sense of urgency
Link that leads you to another page to enter personal information.

Other Phishing Resources

- Video: Phishing Scams in Plain English
- Scams and Schemes - Common Sense Education
- Better Business Bureau Scam Tips
- Game: Phishing Scams - Avoid the Bait

URL Analysis

URL Analysis

- Most email or text message phishing attacks start with a specially-crafted URL.
- Even if an email or text doesn't have any of the phishing features, you can still get hooked!

URL Analysis

- Which URL do you think is the real Facebook URL?
  - https://www.accounts.facebook.com/verifylogin/user/
  - https://www.facebook.fblogin.com/home
- If you read the URL #2 from left to right, like English, then this URL appears legitimate.
- This is the **wrong** way to read a URL.

URL Analysis

- The **right** way to read a URL is right to left.
- FIRST, start on the right of the URL and locate the Top Level Domain (.com)
- The Domain name after the Top Level Domain is the registered user of the website.
  - https://www.accounts.**facebook.com**/verifylogin/user/
  - https://www.facebook.**fblogin.com**/home

Analyze Phishy URL's

- http://bankofthevvest.com **Bad URL**
- https://getsupport.apple.com/?caller=home&PRKEYS= **Good URL**
- http://snapchat.verification.com **Bad URL**
- http://instagram.privacy-information.socialapp.com **Bad URL**

One More Example

Account Suspended Inbox x

First National Bank <service@firstnational.com>
to

4:29 PM (4 hours ago)

First National Bank
One with You.®

Suspicious Login Detected

[redacted]

For security reasons, we're suspending your First National Bank® account(s) as a result of suspicious login activities to your account(s). Until we are able to verify your last login activities, pending and future transactions are suspended.

To verify and regain access to your account, Please **LOGIN NOW** and follow the instructions.

If you don't verify this within the next 24 hours, your account(s) may be closed and your balance - plus all interest earned will be lost.

Sincerely,

Customer Service

Email ID: 327

[redacted]

This email was sent to you as part of the services of FNBO. If you have received this email in error, please ignore.

P.O. Box 3707, Omaha, NE 68103-0707

One More Example