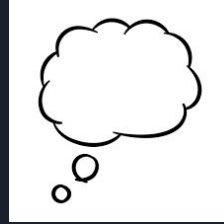


# Phishing



Healthy Steps Hawaii

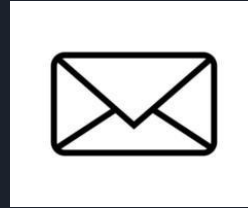
# What is Phishing?



- A cyberattack where an adversary impersonates a legitimate entity such as a boss or employee to deceive individuals into divulging sensitive information, such as passwords or credentials
- The main goal is often identity theft, financial fraud, or unauthorized access to systems such as a corporate network
- Leading cause in data breaches, and company financial losses

# Common Phishing Methods

- **Email Phishing**
  - Fraudulent emails
    - Impersonating co-workers or bosses
    - Scam emails
    - Almost identical looking emails
- **Smishing**
  - SMS Phishing
    - Text Messages
    - Direct messages on social media
- **Vishing**
  - Voice Phishing
    - Attackers impersonate over phone calls
    - Scam calls

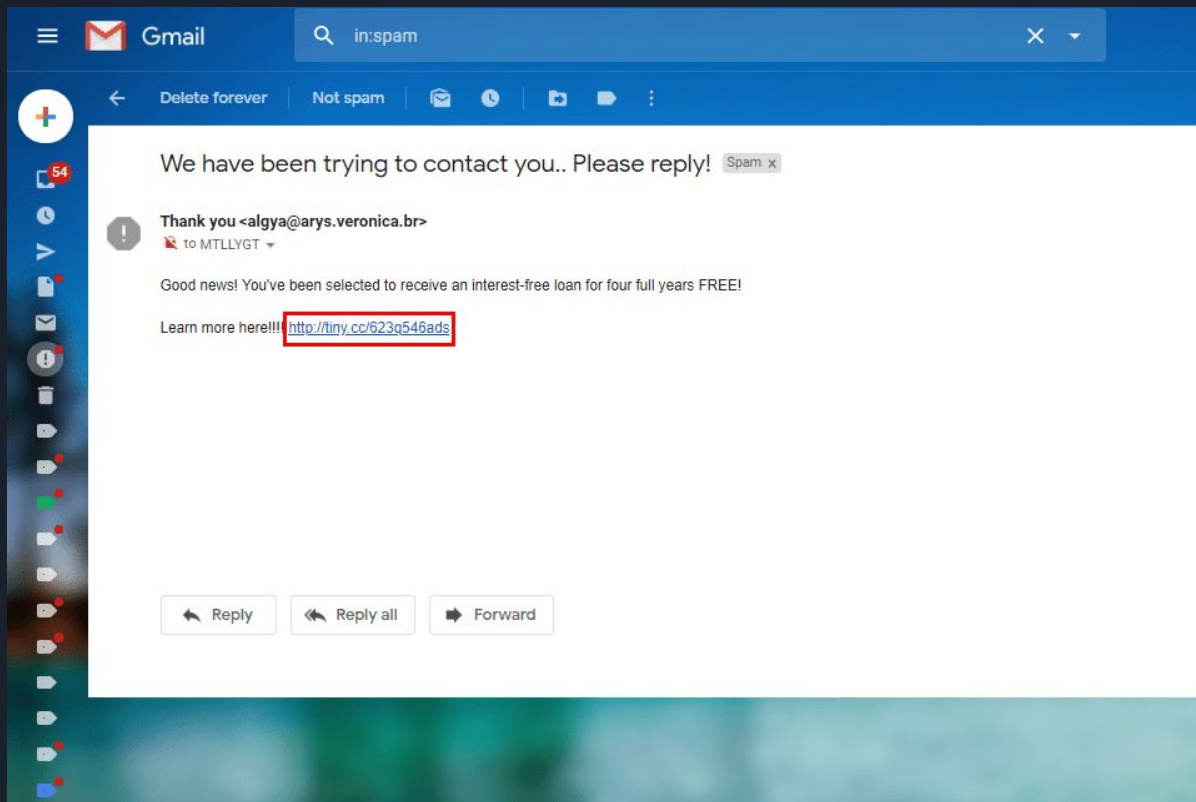




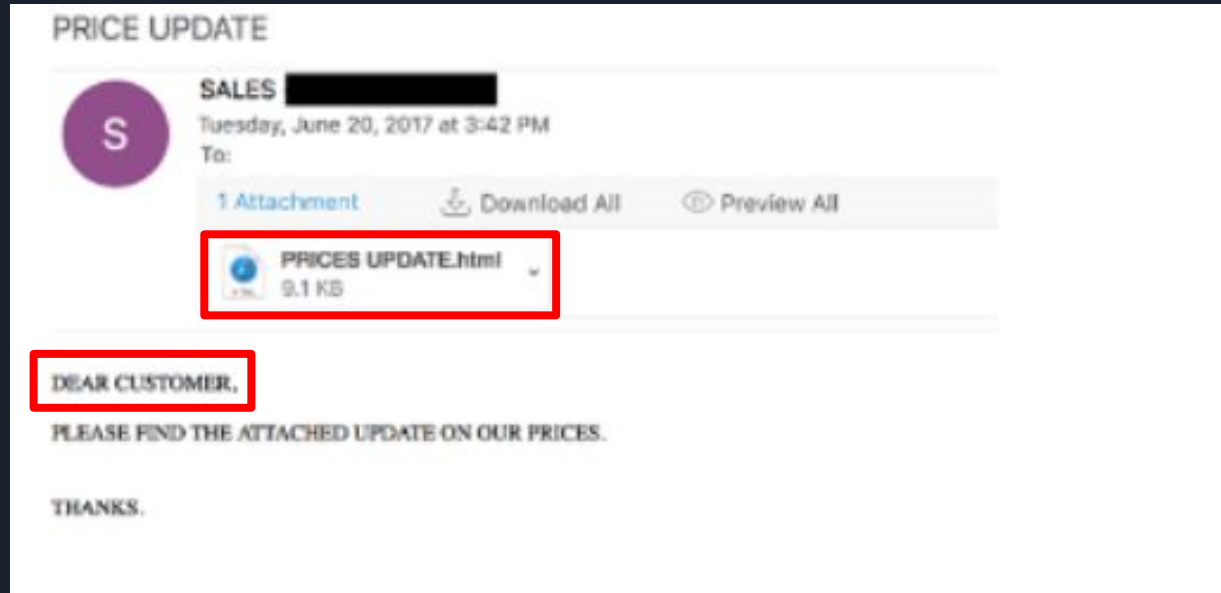
# Recognizing Phishing Attempts

- **Suspicious Links**
  - Hover over email links to verify authenticity of the link
  - Shortened URLs
    - Bitly & TinyURL
    - .xyz, .info, .info, .online endings
- **Urgent Language**
  - Messages that create a sense of urgency
    - “Click now!”
    - “Limited time offer!”
    - “Free!”
- **Generic Greetings**
  - Undirected addressing
    - No specific name mentioned or generic wording such as “customer”
- **Unusual Attachments**
  - Additional files or attachments
    - zip, rar, DOCX, XLS
  - Prompts to download
- **Inconsistent Branding**
  - Logos or elements are poor
    - Inconsistent language
  - Most companies do not ask for additional information
- **Poorly Written**
  - Bad grammar, weird phrasing
  - Odd characters or speech that does not align with the sender

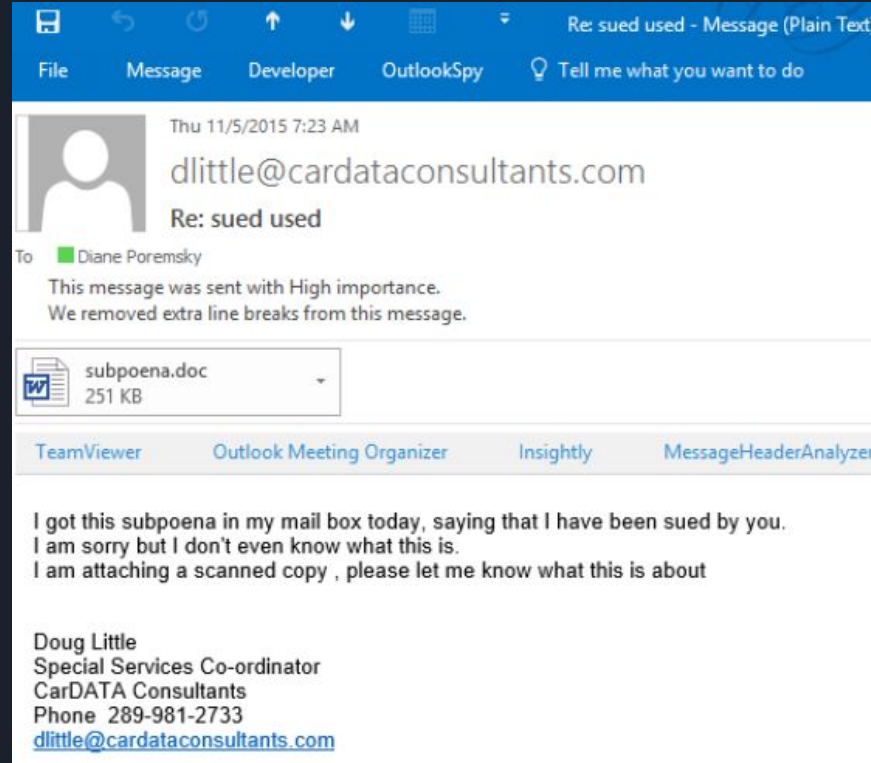
# Examples: Suspicious Link & Urgent Language



# Examples: Generic Greeting & Additional Attachment



# Examples: Try and spot errors!



The screenshot shows an Outlook email window with a blue ribbon at the top. The ribbon includes tabs for 'File', 'Message', 'Developer', 'OutlookSpy', and a search bar 'Tell me what you want to do'. The email header shows the subject 'Re: sued used - Message (Plain Text)' and the date 'Thu 11/5/2015 7:23 AM'. The sender is 'dlittle@cardataconsultants.com' with a profile picture placeholder. The recipient is 'Diane Poremsky'. The message body contains a note about high importance and a removed line break. An attachment 'subpoena.doc' (251 KB) is shown. Below the attachment, there are several toolbars: 'TeamViewer', 'Outlook Meeting Organizer', 'Insightly', and 'MessageHeaderAnalyzer'. The main text of the email reads: 'I got this subpoena in my mail box today, saying that I have been sued by you. I am sorry but I don't even know what this is. I am attaching a scanned copy , please let me know what this is about'. The signature block includes 'Doug Little', 'Special Services Co-ordinator', 'CarDATA Consultants', 'Phone 289-981-2733', and the email address 'dlittle@cardataconsultants.com'.

Re: sued used - Message (Plain Text)

File Message Developer OutlookSpy Tell me what you want to do

Thu 11/5/2015 7:23 AM

dlittle@cardataconsultants.com

Re: sued used

To Diane Poremsky

This message was sent with High importance.  
We removed extra line breaks from this message.

subpoena.doc  
251 KB

TeamViewer Outlook Meeting Organizer Insightly MessageHeaderAnalyzer

I got this subpoena in my mail box today, saying that I have been sued by you.  
I am sorry but I don't even know what this is.  
I am attaching a scanned copy , please let me know what this is about

Doug Little  
Special Services Co-ordinator  
CarDATA Consultants  
Phone 289-981-2733  
[dlittle@cardataconsultants.com](mailto:dlittle@cardataconsultants.com)

# Examples: Try and spot errors!

- High importance precedent
- Suspicious .doc attachment
- Poor grammar, no formal addressing, urgency in message using a subpoena

The screenshot shows an Outlook email window with the following details:

- Subject:** Re: sued used - Message (Plain Text)
- Sender:** dlittle@cardataconsultants.com
- Recipient:** Diane Poremsky
- Attachments:** subpoena.doc (251 KB)
- Body Text:**

I got this subpoena in my mail box today, saying that I have been sued by you. I am sorry but I don't even know what this is. I am attaching a scanned copy , please let me know what this is about
- Signature:** Doug Little, Special Services Co-ordinator, CarDATA Consultants, Phone 289-981-2733, dlittle@cardataconsultants.com

Red boxes and arrows highlight the following elements:

- A box around the text: "This message was sent with High importance. We removed extra line breaks from this message."
- A box around the attachment: "subpoena.doc 251 KB"
- A box around the main body text of the email.



# How to protect yourself

- **Verify Sources**
  - Confirm authenticity through additional methods
    - i.e hover over links, check file typing, confirm with sender
  - Ensure you are expecting communication through a specific channel
    - i.e phone call, email, text
- **Use Multi-Factor Authentication (MFA)**
  - Extra layer of security through outside means
    - Authenticator app on phone
    - Code sent to email
    - Text to phone
    - Phone call to specific number
- **Update Software**
  - Always make sure software is up to date!
  - Install stable or newest versions of software
- **Ensure Intent**
  - If anticipating communication, make sure it comes through proper channels
    - I.e work attachments from company email, personal attachment through verified email domain (gmail, yahoo, hotmail), organization or government through .org, .gov websites.



# Tools and Resources



- **Anti-Phishing Toolbars**

- Toolbar extensions for web browsers that check common phishing sites, attachments or naming conventions

- **Useful websites**

- <https://urlscan.io/>

- Scans urls against common methods of phishing and scams

- <https://www.virustotal.com/gui/home/upload>

- File scanning website to verify website links or check if files contain malware or additional baggage

- **Official Websites**

- Use official websites and platforms for downloads or communication, rather than links through emails or texts

# Stay Vigilant!



- Phishing is difficult to combat as it is always evolving and new methods are created
- Recognize signs from common checks when determining if something is malicious
- Anyone can be susceptible to attacks, no one is truly immune
- Nothing is ever “free” on the internet; if it is too good to be true, it's probably fake
- Even the largest enterprises with robust cyber defense still fall victim to simple phishing tactics, all it takes is a single person to fall victim for it to fall apart



# Sources

- Creatives, A. S. (n.d.). *Download free vectors, images, photos & videos*. Vecteezy.  
<https://www.vecteezy.com/>
- *7 red flags to alert you to a potential phishing scam*. Enterprise Information Technology Services. (n.d.).  
<https://eits.uga.edu/stories/sevenwaystoidentifyaphishingscam/>
- O'Donnell, A. (2023, October 23). *How to test a suspicious link without clicking it*. Lifewire.  
<https://www.lifewire.com/how-to-test-a-suspicious-link-without-clicking-it-2487171>
- *5 ways to spot a phishing email: Envista forensics*. 5 Ways to Spot a Phishing Email | Envista Forensics. (n.d.).  
<https://www.envistaforensics.com/knowledge-center/insights/articles/how-to-spot-a-phishing-email/>