

District Leader Phishing Prevention Guide



Contents

Phishing Prevention Guide	1
Phishing Attacks Explained	2
What is Phishing?	2
How does it work?	2
1. Getting you to click	2
2. Taking you to a fake website	2
What makes the message seem trustworthy?	3
1. Phishing	3
2. Spear Phishing	4
Preventing Phishing Attacks	5
1. Check the e-mail address. Is this someone that you recognize?	5
2. Check the link before clicking. Does it make sense?	5
3. Check for other common Phishing red flags.	6
4. If unsure, verify with the known person or organization.	6
5. Never download suspicious attachments.	6
What to do Next?	7
Phishing Prevention	7
Quick Reference Guide	8
Prevention Steps	8

Phishing Attacks Explained

What is Phishing?

A sophisticated technique used to trick you into allowing access to sensitive information which you would not knowingly provide, such as:

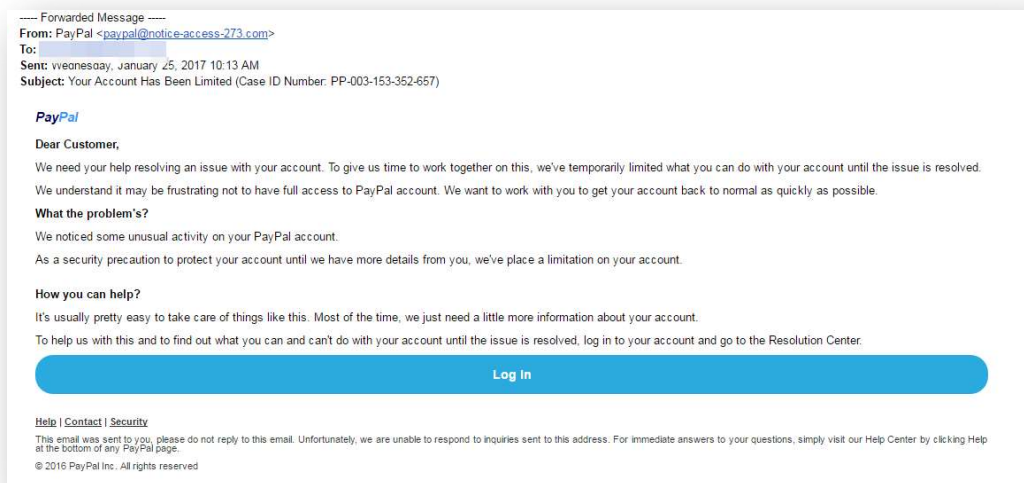
- Your login credentials.
- Access to your personal email account.
- Access to your personal computer.
- Confidential member information.
- Financial information or actual funds.

How does it work?

Almost all attacks fall into 2 scenarios.

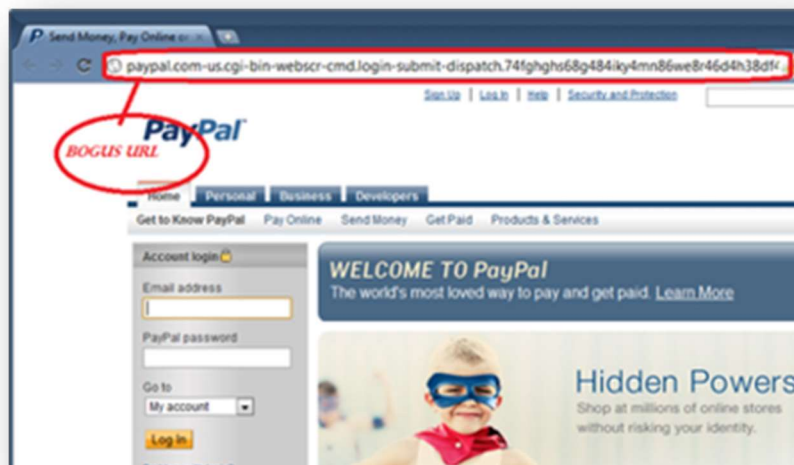
1. Getting you to click

The fraudster you a **compelling message** that appears to come from a **recognizable source**. The message entices you to click a link or open a file, enabling the fraudster to **install malware** aimed at allowing them access to sensitive information on your computer, or to record your keystrokes.



2. Taking you to a fake website

The fraudster sends you a compelling message, which likely also appears to come from a trusted source. The message draws you to a **data harvesting site** that they've created, which also appears to you to a site belonging to your **trusted source**.



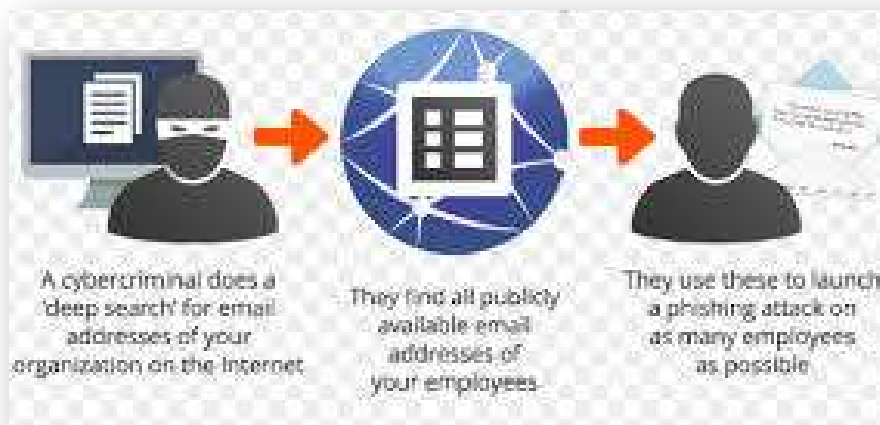
What makes the message seem trustworthy?

Fraudsters have developed sophisticated methods over time to trick you into believing that they're someone that you recognize. These fall into 2 categories.

1. Phishing

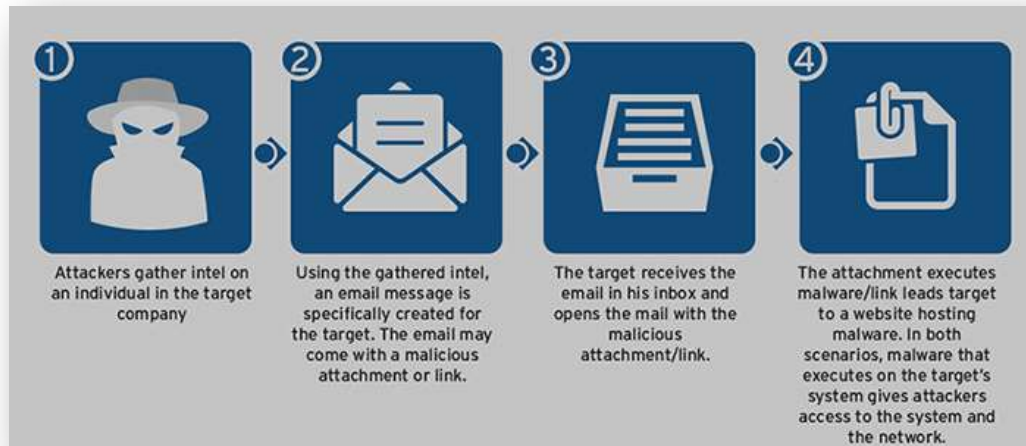
The fraudster sends out a mass message, and your inbox is on the list. Typically, these messages will appear to originate from an organization that you have ties to, such as a bank or volunteer organization.

Often, these fraudsters will perform a deep search for the email addresses of individuals working for or associated with an organization. They will then use these email addresses to launch an attack.



2. Spear Phishing

The fraudster sends you a message which appears to originate from a specific person whom you already know – even their actual email address. They focus on a targeted set of individuals and use social engineering techniques to convince you that you're taking an everyday or urgent course of action.



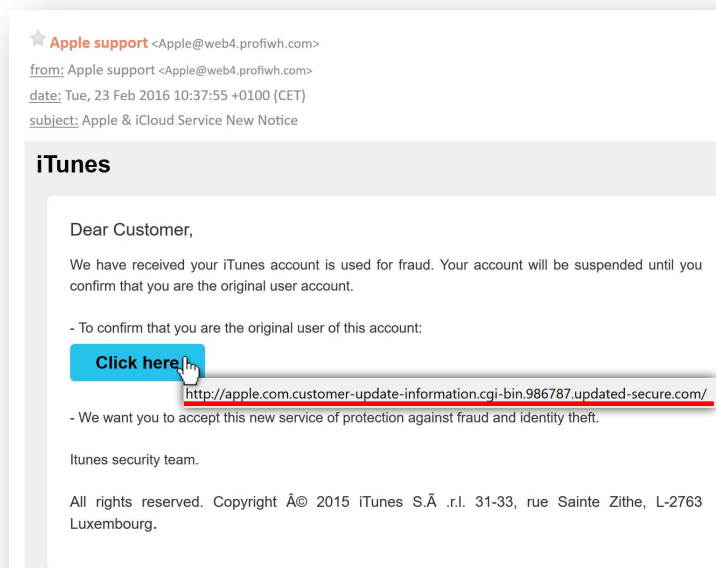
Preventing Phishing Attacks

If an email is prompting you to click on a link or take any action on a site, it is your responsibility to take the following steps to prevent the disclosure of sensitive information.

1. Check the e-mail address. Is this someone that you recognize?
 - Never trust the name. Instead, check the entire email address.
 - Look carefully at what comes after the @ sign. For example, is it @toastmasters.org or @toastmasterswhq.org?



2. Check the link before clicking. Does it make sense?
 - Hover your mouse over the link to see the site it will lead you to.
 - Is the URL spelled correctly?
For example, is it toastmasters.org or toastmusters.org?
 - Do you recognize the URL?
In the below example, the correct URL for iTunes is not apple with a lengthy extension, enabling the recipient to recognize it as a phishing attempt.



- If you're still unsure, right click and copy the link. Go to an web evaluator site such as <https://safeweb.norton.com/> and use it to test the link's validity.

3. Check for other common Phishing red flags.


- The email indicates that there is an urgency such as a pending deadline which you weren't anticipating previously (such as an expiring insurance policy).
- There is an offer of large financial rewards.
- Content full of warnings or potential consequences.
- Suspicious use of words, spelling, or grammar.



4. If unsure, verify with the known person or organization.

- Call or send a separate email to the person you know to ask if they sent you the link, file or document.
- Instead of using the link in the email, enter the URL you already know into your browser and check the website directly.

5. Never download suspicious attachments.



What to do Next?

As A Member

1. Be careful and attentive when checking your email.
2. If you receive a phishing attempt, delete it.
3. If you receive a phishing attempt that is associated with Toastmasters, please notify phishing@toastmasters.org, then delete it.

As A Leader

1. Be careful and attentive when checking your email.
2. Do not store member information offline.
3. Set secure passwords to protect member information.
4. If you receive a phishing attempt, delete it.
5. If you receive a phishing attempt that is associated with Toastmasters, please notify phishing@toastmasters.org, then delete it.
6. If you feel the need to communicate with members regarding potential phishing, please communicate with the Districts team at districts@toastmasters.org first.

Phishing Prevention

Quick Reference Guide

Prevention Steps

1. Check the **email address**.
2. Check the **link** before clicking.
3. Check for other **common red flags**.
 - a. Communicates urgency or a pending deadline.
 - b. Offers financial rewards.
 - c. Warnings of potential consequences.
 - d. Suspicious use of words, spellings, or grammar.
4. If unsure, **verify** with the known person or organization.
5. **Never download** suspicious attachments.

I suspect or have fallen for a phishing attempt. What do I do now?

1. Do not reply to or forward the email.
2. Do not click on any links in the email.
3. Do not download any attachments in the email.
4. Notify phishing@toastmasters.org of any Toastmasters-related phishing attempts.
5. Delete the email.