



Is an e-mail legitimate?

Information and examples on what to look for

Computing & Information Technology (C&IT) receives many reports about suspicious looking e-mails that Wayne State University students, faculty, & staff receive on a regular basis.

The e-mail message looks like it is being sent from “Wayne Webmail support,” “Webmail Administrator,” “Wayne messaging center,” or “THE WAYNE DESK,” among others. The message asks you to forward your e-mail password and/or other personal information. C&IT will *never* ask you for this information.

If the senders of these messages receive the information they need from you, it is possible:

- They can gain access to the organization’s entire computer network.
- They could access your account on computer systems like WSU Pipeline and the Banner Administrative System. This would put your personal information stored on these systems at risk.
- They can also use your e-mail address for spamming purposes, in which case you receive spam messages, or messages are spoofed to look like you sent them.

If you click an unknown or fake link in the message, scammers can install malware (malicious software), or spyware, onto your computer. The spyware can record keystrokes for the scammer so they can obtain passwords to sensitive material or accounts.

The technique these scammers use is called social engineering. Their intention is to induce panic in you after you read the e-mail. You may be so distracted that you reply immediately without a second thought. Phishing e-mails follow similar patterns. The message states there is a problem with your account, whether it be your WSU E-mail account, bank account, or PayPal account (even if you don’t have a PayPal account), for example.

Usually the e-mail notes a penalty for not responding to the message, such as “your account will be closed or suspended.” Again, scammers are trying to induce panic in you, so

you believe something is wrong and will give them the information they want.

Delete these e-mail messages immediately. Never share your account password with anyone.

If you are ever in doubt as to whether the content is legitimate, contact the C&IT Help Desk or the bank, company, or organization directly.

You can report phishing attacks at WSU by filling out a form here:

<https://calltracker.wayne.edu/phishreport/>

The following pages include examples of phishing e-mails WSU students, faculty, and staff have received. You may have seen some of them yourself, and if you deleted them, you did the right thing.

Please review the examples for what to look for in an e-mail to determine whether it is legitimate or not.

Remember, sending any users IDs, passwords, or other personal information to a stranger, puts yourself and others at risk!

If you did happen to reply, contact the appropriate organization immediately. If you replied to what you believe is a phony WSU e-mail, contact the C&IT Help Desk by phone at (313) 577-4778 or by e-mail at helpdesk@wayne.edu.

Table of Contents

Fake WSU WebMail Example 1	2
Fake WSU WebMail Example 2	3
Fake WSU WebMail Example 3	4
Fake American National Bank of Texas E-mail...	5
Fake Internal Revenue Service E-mail	6
Fake PayPal E-mail	7
Conclusion	8

What to look for: You receive an e-mail message where the sender is confirming account information.

The example e-mail message below says all unused “webmail” accounts will be deleted, and, to prevent yours from closing, you must reply immediately to confirm your account information.

These statements are social engineering techniques used to “induce panic” in you so you reply without a second thought. C&IT will never ask you for your account information.

The screenshot shows an email client window titled "Confirm Your School Webmail Accou... M". The email header shows it is from "Webmail Admin Support Team [info@websupport.com]" sent on "Fri 7/11/2008 6:32 AM" to "undisclosed-recipients". The subject is "Confirm Your School Webmail Account Details". The body of the email is in a monospaced font and contains the following text:

Dear Account User,

This message is from webmail messaging center to all webmail account owners. We are currently upgrading our data base and e-mail account center. We are deleting all unused webmail account to create more space for new accounts.

To prevent your Account from closing you will have to update it by providing the information requested below:

Confirm Your Account Details
Webmail ID:
Password:
DOB:

You will be sent a new confirmation alphanumerical password so that it will only be valid during this period and can be changed after the process.

Thanks for your understanding.
Webmail Administrator.

Warning!!! Account owner that refuses to update his or her account within seven days of receiving this warning will lose his or her account permanently

Annotations with arrows pointing to specific parts of the email:

- The e-mail is not from Wayne State University. "Webmail Admin Support Team" and "websupport.com" were added to help the e-mail seem official.** (Points to the "From:" field)
- The e-mail is not addressed to you directly.** (Points to the "To:" field)
- Note the typo.** (Points to "data base" in the body text)
- Several statements induce panic: -"We are deleting all unused webmail accounts." -"To prevent your account from closing..."** (Points to the threatening statements in the body)
- You are being asked to provide personal information. C&IT will never request this from you.** (Points to the list of requested information: Webmail ID, Password, DOB)
- Note the inconsistent punctuation.** (Points to the missing period after "Thanks for your understanding.")

Delete this e-mail immediately, or when in doubt, fill out the WSU Phishing Report form at:
<https://calltracker.wayne.edu/phishreport.php>

What to look for: You receive a poorly written e-mail message full of inconsistent information.

The e-mail message below is written very poorly. It contains multiple spelling and punctuation errors and sentences that do not make sense.

This message uses a security upgrade as an excuse to get you to reply with your e-mail password. This is common in phishing attempts. Remember that, as soon as you read a statement requesting personal information, you can safely delete the message.

The screenshot shows a webmail window titled "UP-GRADE YOUR EMAIL ACCOUNT — Random". The header information is as follows:

- From: THE WEBMAIL.WAYNE.EDU SUPPORT TEAM <users-account@wayne.edu>
- Subject: UP-GRADE YOUR EMAIL ACCOUNT
- Date: July 5, 2008 9:33:11 PM EDT
- Reply-To: webupgrade1@gmail.com

The body of the email contains the following text:

Dear valued customer,

We are currently performing maintenance for our Digital Webmail Customers. We intend upgrading our Digital Webmail Security Server for better online services.

In order to ensure you do not experience service interruption, Please you must reply to this email immediately and enter your password here(*****) and Check out your new features and enhancements with your new and improved wayne.edu account, To enable us upgrade your wayne.edu Account for better online services please reply to this mail.

Thank You for Using ueg.br account

Annotations in red boxes point to the following elements:

- Note: Reply-To address is a gmail account.** (Points to Reply-To: webupgrade1@gmail.com)
- You are not addressed by your name.** (Points to Dear valued customer,)
- The message says you must reply "immediately", which is a way of inducing panic in you so you will respond.** (Points to "must reply to this email immediately")
- The closing statement does not match content within the message. The spammers are inconsistent and are thanking you for "Using" a strange account.** (Points to Thank You for Using ueg.br account)
- Scammer is spoofing the e-mail address so it looks as if it is coming from a WSU source.** (Points to From: THE WEBMAIL.WAYNE.EDU SUPPORT TEAM)
- You are being asked to provide personal information. When you receive an e-mail containing such a request - delete it immediately. C&IT will never request account information.** (Points to the password request section)

Delete this e-mail immediately, or when in doubt, fill out the WSU Phishing Report form at:
<https://calltracker.wayne.edu/phishreport.php>

What to look for: You receive an e-mail from a familiar institution, but the content contains many misspellings. Phishing e-mails tend to contain misspelled words or punctuation mistakes. The message below misspells “Wayne” throughout the e-mail (spelled “WAYANE”).

In addition, the message requests personal information from you. It also states that your account will be deleted in seven days if you don't send your information.

These are social engineering techniques scammers use to induce panic in you. An e-mail scam that targets employees in particular is known as “spear phishing.”

The image shows a screenshot of a webmail interface for a 'Dear WAYANE.EDU Email Account Owner' email. The interface includes a header with window controls and navigation buttons (Delete, Junk, Reply, Reply All, Forward, Print, To Do). The email content is as follows:

From: WAYANE Team WAYANE.EDU beta <info@verification.com>
Subject: Dear WAYANE.EDU Email Account Owner
Date: April 27, 2008 7:18:09 PM EDT
Reply-To: upgrade_team@uymail.com

Dear WAYANE.EDU Email Account Owner,

This message is from WAYANE.EDU messaging center to all WAYANE.EDU email account owners.

We are currently upgrading our data base and e-mail account center. We are deleting all unused WAYANE.EDU email account to create more space for new accounts.

To prevent your account from closing you will have to update it below so that we will know that it's a present used account.

CONFIRM YOUR EMAIL IDENTITY BELOW Email
Username :
Email Password :
Date o Birth:.....
Country or Territory :

Reply to the support team below:
Mr Harword Hanks
E-mail: upgrade_team@uymail.com

Warning!!!

Account owner that refuses to update his or her account within Seven days of receiving this warning will lose his or her account permanently.

Thank you for using WAYANE.EDU !
Warning Code:VX2G99AAJ Thanks,
WAYANE Team WAYANE.EDU beta

Callout boxes with arrows pointing to specific elements:

- Reply-To address is different than the From address, and it is not associated with WSU.** (Points to the Reply-To field)
- You are being asked to provide personal information. When you receive an e-mail containing such a request - delete it immediately. C&IT will never ask you for this kind of information.** (Points to the form fields)
- You are not being addressed directly in the salutation.** (Points to the salutation)
- "Wayne" is spelled as "WAYANE" throughout the e-mail.** (Points to the subject and body text)
- Beware of multiple warnings that you will lose your account if you do not provide the requested information.** (Points to the warning text)
- It is signed "WAYANE Team" to help it look legitimate.** (Points to the signature)

Delete this e-mail immediately, or when in doubt, fill out the WSU Phishing Report form at:
<https://calltracker.wayne.edu/phishreport.php>

What To Look for: You receive an e-mail from a financial institution where you do not have an account.

Social engineering applies to this message as well. The subject reads "Security Alert" in an attempt to induce panic in you. The message also has no other details except that the "Message Center" on the bank's Website has a message waiting for you, and the only way to view it is by clicking the included link. This is the scammer's way of luring you to click the link. If you are unsure of the legitimacy of a link in a message, do not click it.

It is safe to assume that any reputable organization would not contact you via e-mail regarding an important matter. If you are ever in doubt, contact the institution directly by calling a customer service telephone number.

The e-mail is not addressed to you directly.

Random letters are included in the e-mail subject line for no apparent reason.

Note the font changes within the message. The scammer may be copying and pasting content from other phishing messages or from pages on the institution's Website.

The actual Web address is revealed when you place your cursor over the link. The "anbtx" portion of the address was added to help the message look legitimate. Technically it does not go to the American National Bank of Texas Website.

Message Details:
 From: American National Bank of Texas [trust@anbtx.com] Sent: Tue 7/15/2008 7:03 AM
 To: undisclosed-recipients:
 Cc:
 Subject: Security Alert!! ID: RTHHRRDHWD

Message Content:
 You have 1 new ALERT message
 Please login to your **American National Bank of Texas Online Login** and visit the **Message Center** section in order to read the message.
 To Login, please click the link below:
<http://mail.actionhousing.org/online/www.anbtx.com/>
 Click to follow link
 American National Bank of Texas Online Banking
 Copyright © 2008 American National Bank of Texas

Delete this e-mail immediately, or when in doubt, fill out the WSU Phishing Report form at:
<https://calltracker.wayne.edu/phishreport.php>

What to look for: You receive an e-mail that the IRS owes you money. You can safely assume the IRS would not be contacting you via e-mail.

A couple social engineering techniques are being used in the sample message below. The scammer wants you to believe a tax refund of \$500 is waiting for you, but you only have so many days to claim the money. A statement in bold red type reads "... wrong inputs will be prosecuted by law," and a copyright statement closes the e-mail. These are attempts to make the e-mail look official.

Again, when in doubt, contact the institution directly.

The image shows a screenshot of an email client window titled "Get your tax refund now - Messag...". The email header shows it was sent from "Internal Revenue Service" with the address "[yourtaxrefund@InternalRevenueService.com]" on Tuesday, 7/22/2008 at 10:37 AM. The subject is "Get your tax refund now". The body of the email contains the following text:

This message was sent with High importance.
This message has extra line breaks.

From: Internal Revenue Service
[yourtaxrefund@InternalRevenueService.com] Sent: Tue 7/22/2008 10:37 AM

To:
Cc:
Subject: Get your tax refund now

After the last annual calculations of your account activity we have determined that you are eligible to receive a tax refund of **\$479.30**. Please submit the tax refund request and allow us 2-6 days in order to process it.

A refund can be delayed for a variety of reasons. For example submitting invalid records or applying after the deadline.

To access the form for your tax refund, please click [here](http://e-dlogs.rta.mi.th:84/www.irs.gov/).

Note: Deliberate wrong inputs will be prosecuted by law.

Regards,
Internal Revenue Service

© 2008, Internal Revenue Service United States Department of the Treasury.

Annotations with arrows point to various parts of the email:

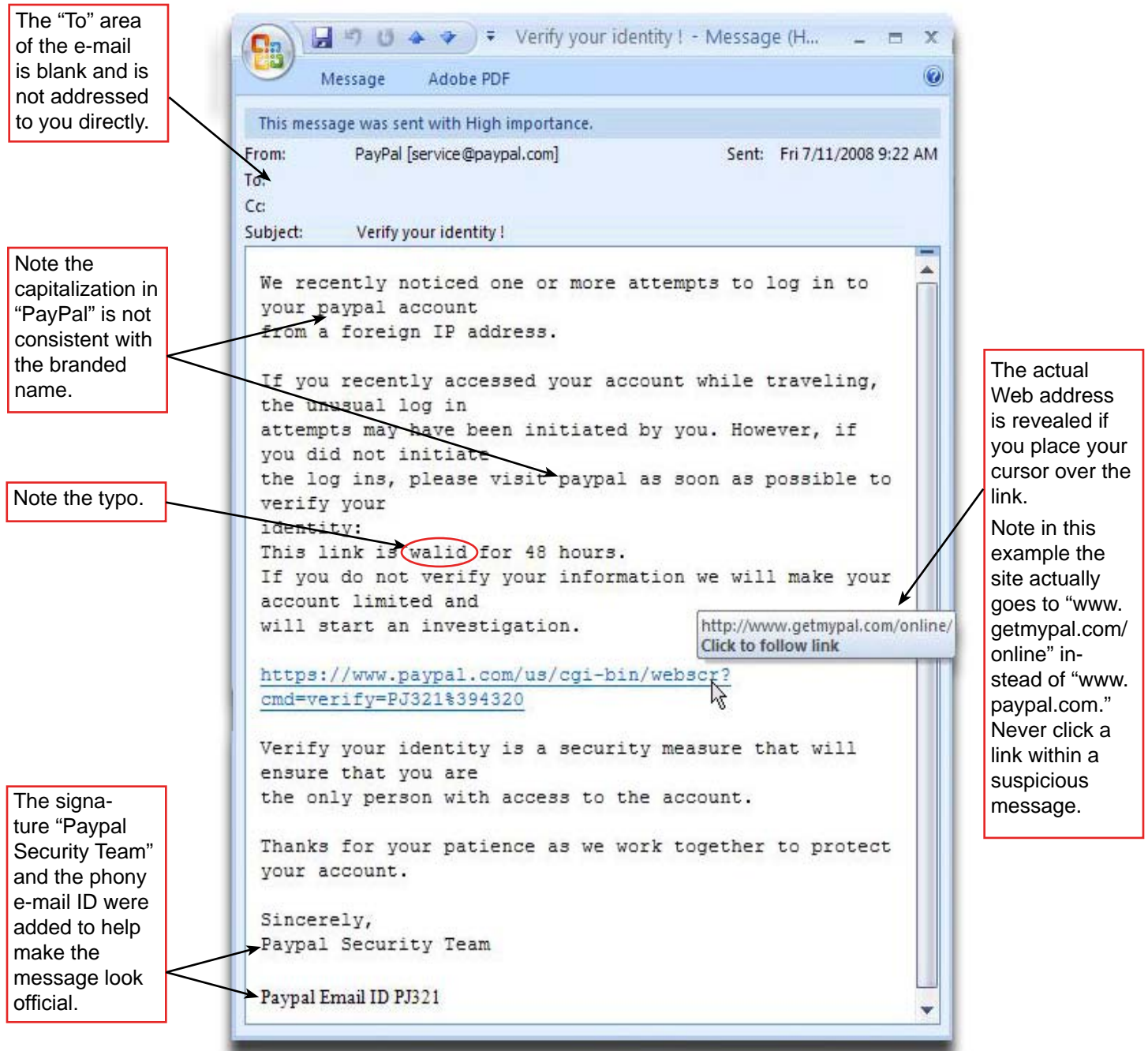
- This e-mail address was added to help it look official.** (Points to the sender's email address)
- The "To" field is blank and the message is not addressed to you directly.** (Points to the empty To and Cc fields)
- You are being told a tax refund is waiting for you, yet your name does not appear anywhere in the e-mail.** (Points to the body text)
- You are being lured to click a link.** (Points to the "here" link)
- The actual Web address is revealed when you place the cursor over the word "here."** (Points to the tooltip showing the URL: http://e-dlogs.rta.mi.th:84/www.irs.gov/)
- Note the link actually points to a site not associated with the IRS, and the "www.irs.gov" portion was added to help the e-mail seem legitimate.** (Points to the URL tooltip)
- These statements are added to help the message look official.** (Points to the bold red note and the copyright footer)

Delete this e-mail immediately, or when in doubt, fill out the WSU Phishing Report form at:
<https://calltracker.wayne.edu/phishreport.php>

What To Look for: You receive an e-mail from PayPal to verify your identity. This is a popular scam, and it is sent to everyone, not just those with PayPal accounts.

This particular scam wants you to believe that someone other than you has been trying to access your account.

You may even receive an e-mail about a PayPal account you do not have. Any reputable organization like PayPal would not ask you to provide this information within an e-mail.



Delete this e-mail immediately, or when in doubt, fill out the WSU Phishing Report form at:
<https://calltracker.wayne.edu/phishreport.php>

The communications staff in C&IT prepared this document, and the examples in it, to help you learn how to determine whether an e-mail is legitimate.

Remember the following tips to better protect yourself from e-mail scams:

- Never reply to an e-mail message requesting a password, user name, account number, or any personal or financial information — no matter how legitimate the message may seem or who appears to have sent it. Be assured that WSU will never ask you to e-mail your computer account password or other personal information. Delete the message.
- If you are not a member of the organization that is supposedly sending the e-mail, delete it.
- Never click a link inside an e-mail if you do not recognize the Web address or cannot tell where it will take you.
- Run software programs like anti-virus and anti-spyware and keep them up to date. WSU students, faculty, and staff can download Symantec Antivirus for free through the Software Clearinghouse at:
<http://clearinghouse.wayne.edu/currentsite/downloads.htm>
- Knowledge is power. Familiarize yourself with phishing techniques so you can easily spot a fake e-mail. Review the information about phishing on C&IT's Website:
<http://computing.wayne.edu/security/phishing.php>
- Report suspicious e-mails to C&IT by filling out the WSU Phishing Report form:
<https://calltracker.wayne.edu/phishreport.php>
- If you replied to what you believe is a phishing attempt at WSU, contact the C&IT Help Desk at (313) 577-4778 or e-mail helpdesk@wayne.edu. If you responded to what you believe is a phishing attempt regarding your personal bank account, contact the bank or financial institution directly.

WAYNE STATE
UNIVERSITY

COMPUTING & INFORMATION
TECHNOLOGY