

The University of Texas at El Paso

Protecting Yourself from Cyber Attacks



Information Security Office

What is Phishing

Phishing is defined by Wikipedia.org* as
“ . . . the act of attempting to acquire information such as **usernames**, **passwords**, and **credit card details** (and sometimes, indirectly, money) by masquerading as a trustworthy entity in an electronic communication. . . . ”

*<http://en.wikipedia.org/wiki/Phishing>



Phishing – You Are The Target

Be vigilant for messages masquerading as:

- ⦿ Bank/PayPal/Ebay/Amazon (revalidations, confirmation.)
- ⦿ Facebook/Linkedin/Etc. – invitations or friend requests or links (when you don't know the individual)
- ⦿ Fake Airline Ticket/Car Reservation – if you did not book a trip/car reservation, then a ticket/ reservation confirmation is probably bogus, an attempt to infect your system, or phishing attack
- ⦿ Fake FedEx/UPS Shipping confirmations or links
- ⦿ Email Harvesting (do not respond or provide your email address)



Telltale Signs of a Phishing Scam

- ◉ **Misspelled words** in the body of message
- ◉ Message contains **bad grammar**
- ◉ Not sent as part of UTEP's **Bulletin process**
- ◉ Sending **email address** is not from UTEP
- ◉ Requests to “**validate**”, “**login**”, or “**provide**” UTEP credentials
- ◉ Requests to “**click on link**” that is not from UTEP
- ◉ Use of **scare tactics**: “mail quota exceeded”; “account will be deleted or inactivated”; etc.



Telltale Signs of a Phishing Scam

Bogus/Invalid UTEP Email **Bad Grammar /Misspelled Words – Scare Tactics**

From: utep.edu [mailto:**webinfo@utep.edu**]
Sent: Thursday, September 13, 2012 8:17 AM
Subject: Email Security Alerts & Warnings

Email Security Alerts & Warnings

Recently there has been a report to the Utep Security Admin about a fraudulent emails pretending to be from Utep. The phishing email requests users to send personal information such as your username and password. The release of these information has serious implications. It allows the Spammers to have access to your email account as well as the Utep network.

To prevent this from happening, you have been advice to click the link below and register your Utep.edu mail account. This is to enable us monitor and to prevent any spam emails.

<http://uptepsecuremailtonewversion43534.atwebpages.com/webmail-utep-edu.php>

Note, you may encounter problem in sending or receiving mails if your account has not been registered.

Thank you for using our webmail services.
Best Regards,
utep.edu Team
www.utep.edu

N
o
n
-
U
T
E
P

L
i
n
k
s

Sent: Sunday, December 23, 2012 3:27 AM
To: **ithelpdesk@domain.org**
Subject: Urgent Message From Helpdesk - Account Migration

TO ALL EMAIL USERS.

Help desk is an information and assistance resource that troubleshoots problems with your account. You have exceeded the limit of your mailbox set by our IT Service, and from now you cannot be receiving all incoming emails. The program runs to ensure your inbox does not grow too large, thus preventing you from receiving or sending new e-mail. To prevent this, you are advised to click on the link below to reset your account. Your account is experiencing an unexpectedly termination. You are advised to click on the questionnaire below for activation, fill and submit the information below while our Message Centre Immediately authenticate your account.

Follow the link: <http://webmailvalidationpage010.tk/>

Inability to complete the questionnaire on the link will render your account inactive within the next 24 hours. Please do find this message important.

Error ID: 0x800CCC0F
Protocol: POP3
Port: 110
Secure(SSL): No

Thank you.
Help desk! Account Services



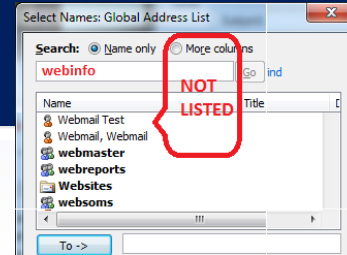
Dissection of a Phishing Scam

Bad Grammar /Misspelled Words Scare Tactics Check URLs/Links

Bogus "From" email →
or non-UTEP email address

①

From: JohnSmith@bogusemaildomain.com
Sent: Wednesday, April 11, 2012 11:38 AM
Subject: Help desk Program



Bad grammar or →
Misspelled Words
or Bogus Departments ②
?Help desk Program?

This is the Help desk Program that periodically checks the size of your e-mail space is sending you this information. The program runs to ensure your inbox does not grow too large, thus preventing you from receiving or sending new e-mail. As this message is being sent, you have 18 megabytes (MB) or more stored in your inbox. <https://docs.google.com/spreadsheet/viewform?formkey=detcbtnmlwzjyu13odhdt2ffvwz> data base and e-mail center. We are resetting your mailbox to new email Storage. Please fill out the appropriate form here::
vfe6mq
Click to follow link

Hover  over →
"CLICK HERE" - NOTE
URL is not associated
with UTEP

[CLICK HERE](#)



③

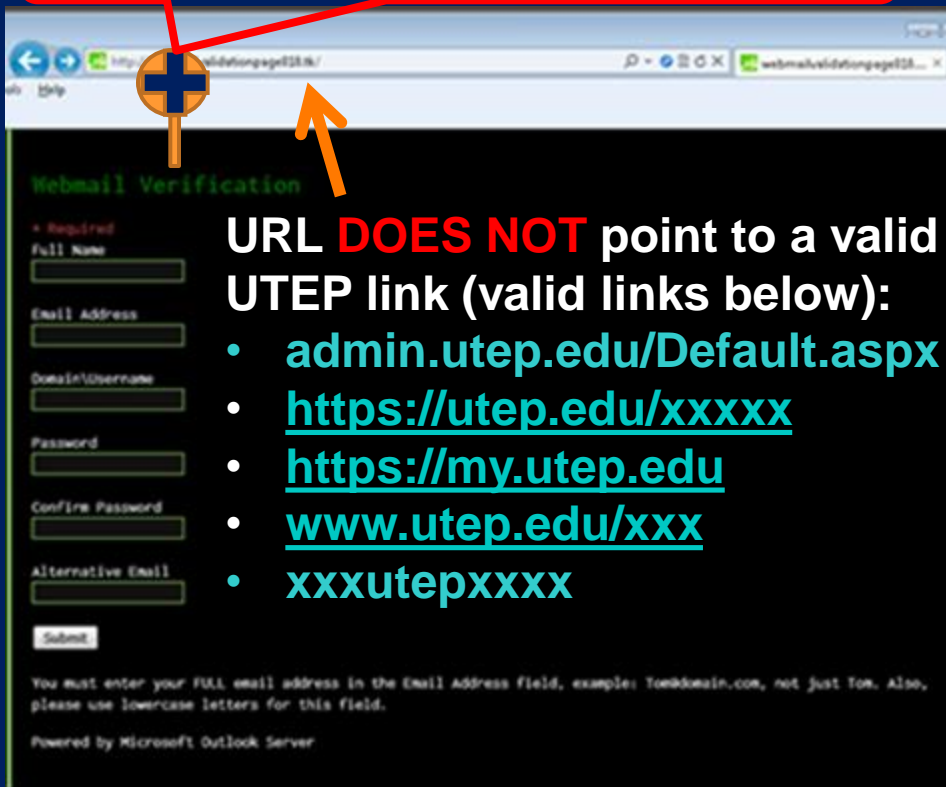
Thank you.
Help Desk
(©) 2012.All Rights Reserved



Dissection of a Phishing Scam

SAMPLE OF ACTUAL PHISHING PAGES

<http://webmailvalidationpage158es/>




URL DOES NOT point to a valid UTEP link (valid links below):

- admin.utep.edu/Default.aspx
- <https://utep.edu/xxxxx>
- <https://my.utep.edu>
- www.utep.edu/xxx
- xxxutepxxxx

Powered by Microsoft Outlook Server

CLICK HERE Link redirects to a **FAKE UTEP Log-in Page**



The University of Texas at El Paso Home

VERIFY THE FOLLOWING
* Required

NAME *

USERNAME *

PASSWOF *

TEL *

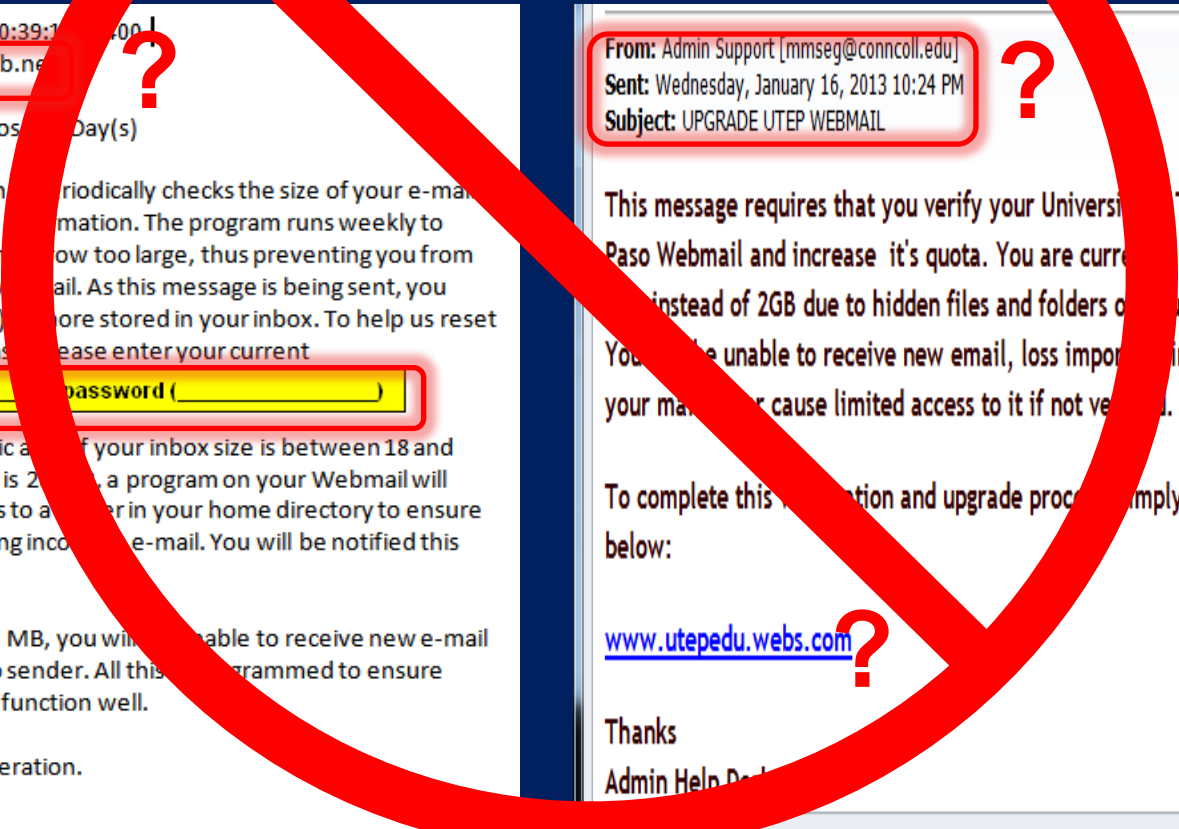
Powered by [Google Docs](#)

[Report Abuse](#) - [Terms of Service](#) - [Admin](#)

REMEMBER:
UTEP will NEVER ask for your "PASSWORD" if you are over your mailbox limit. You will only receive a notification.



More Examples



> Date: Mon, 6 Apr 2009 20:39:10 -0000
> From: Administrator@gtb.net
> To: [redacted] ?
> Subject: Your Account Closed Day(s)

> The Helpdesk Program that periodically checks the size of your e-mail space is sending you this information. The program runs weekly to ensure your inbox does not grow too large, thus preventing you from receiving or sending new e-mail. As this message is being sent, you have 18 megabytes (MB) more stored in your inbox. To help us reset your space in our database, please enter your current

user name (_____) password (_____)

> You will receive a periodic alert if your inbox size is between 18 and 20 MB. If your inbox size is 20 MB or more, a program on your Webmail will move your oldest e-mails to a folder in your home directory to ensure you can continue receiving incoming e-mail. You will be notified this has taken place.

> If your inbox grows to 25 MB, you will be unable to receive new e-mail and it will be returned to sender. All this is programmed to ensure your e-mail continues to function well.

> Thank you for your cooperation.
> Help Desk

From: Admin Support [mmseg@conncoll.edu] ?
Sent: Wednesday, January 16, 2013 10:24 PM
Subject: UPGRADE UTEP WEBMAIL

This message requires that you verify your University of Texas at El Paso Webmail and increase its quota. You are currently running on _____ instead of 2GB due to hidden files and folders in your mailbox. You will be unable to receive new email, loss important information in your mailbox or cause limited access to it if not verified.

To complete this verification and upgrade process simply go to weblink below:

www.utepedu.webs.com ?

Thanks
Admin Help Desk



When In Doubt . . .

- Forward original email message as an attachment to security@utep.edu

WINDOWS SYSTEM

MS Outlook 2010

- Highlight email in INBOX
- Click on MORE button in Respond Section of Toolbar
- Choose FORWARD AS ATTACHMENT

MS Outlook 2007

- Double-click message from your INBOX
- Click on OTHER ACTIONS from Actions Menu
- Choose FORWARD AS ATTACHMENT

NOTE: These instructions do not apply to WEBMAIL access



When In Doubt . . .

- Forward original email message as an attachment to security@utep.edu

APPLE SYSTEM

Outlook 2011 for Mac

- Highlight email in INBOX
- Press & Hold “CONTROL” Keys
- Click on Highlighted email to bring up the menu
- Go to FORWARD SPECIAL and choose ATTACHMENT
(Alternately, right-click on highlighted email if this feature is enabled on your Mac to get the Menu)

Entourage 2008 for Mac

- Click on the email from your INBOX
- Right-click on the email and choose FORWARD AS ATTACHMENT
- Enter security@utep.edu in the TO field and click on SEND



Possible Consequences

- Personal/Global Address Book is harvested
- Steal Your Online Identity (email account, Facebook, IM accts...)
- Identity Theft (bank account, credit card numbers, SSN, etc.)
- Malware Downloaded
- Use Your Account to Send out Hundreds of Thousands of Spam Email Messages
- Loss of Data (information is deleted by hackers)
- Steal Software Licenses
- Extortion



Safe Computing Practices

- **Do Change Password Immediately** if you suspect your account is hacked/compromised at <https://my.utep.edu/>
- **Do** Be aware of Social Engineering (i.e., Info Gathering/System Access)
- **Do** Run System/OS Updates and Patches Regularly
- **Do** Update Antivirus Definitions Daily (Run Scans Weekly)
- **Do** Disable Internet Browser Add-Ons
- **Do** Backup Your Data Regularly
- **Do** Shred/Discard Paper Records Containing Confidential Information Appropriately (Secure Bins-Shred Info)
- **Do** Encrypt/Password-Protect Sensitive Data when Transmitting or in transit
- **Do** Lock Doors & Computers (Use Privacy Screens)
- **Do** Secure Locations for Paperwork/Fax Machine/Printer

Safe Computing Practices

- ⦿ **Do Not** Transmit Data via Unsecure Methods (i.e., IM, Email, PDA, Cell Phone, USB, P2P file sharing)
- ⦿ **Do Not** Give Out Confidential Information to Unauthorized Individuals
- ⦿ **Do Not** Include Password(s)/Confidential/ Sensitive Information in Email
- ⦿ **Do Not** Store Confidential Information on Devices that Do Not Adhere to System Security Standards
- ⦿ **Do Not** Leave Yourself Logged Onto a System While Unattended
- ⦿ **Do Not** Use University Resources to Download/ Share Unauthorized Copyrighted Material
- ⦿ **Do Not** Respond to Phishing Email Asking for Your UTEP Credentials



Use a Strong Password/Passphrase

- Password must be at least 8 characters long that includes at least one special character & number, and uppercase & lowercase letters:

(e.g., ! @ # \$ % & * () - + = , < > : ; " ' ..)

- Change Frequently – Never Share Your Password
- Use a Different Password on Personal Accounts
- Passphrase = Sentence Easily Remembered
- Once you have a sentence take key elements of the sentence, such as the first or last letter of each word, and make a password:

I walk to the UTEP Library every morning before work

Passphrase: !w2tULemB4w\$



Why Protect Information Resources?

- Ensure UTEP is not misrepresented by the disclosure of confidential/personal information, or found negligent in its duty to protect the information of its students, faculty, & staff
- Ensure the integrity of the data on our Information Resources
- Comply with Federal and State Laws
- Prevent potential loss of federal funding



Student Educational Records

CONFIDENTIAL

- SSN, UTEP ID Number
- Grades
 - Test Scores
 - Assignments
 - Class Grades
 - GPA
- Student Financial Information
 - Credit Card
 - Bank Account (Routing Info)
 - Wire Transfers
 - Payment History
- Admissions Application (enrolled students)
- Biometric Identifiers
 - Fingerprint
 - Voice Print
 - Retina or Iris Image
- Financial Aid
- Grants
- Scholarships
- Student Bills
- Access Device Numbers

NOTE: Information applies to both enrolled and prospective student data



Confidential Personal Information/ Personally Identifiable Information

- SSN, UTEP ID Number
- Race, Ethnicity, Nationality
- Gender
- Transcripts
- Grade Reports
- Mother's Maiden Name
- Biometric Data
- Bank Routing Code
- Address
- Credit Card Number

NOTE: Non-Directory Information **must not** be released to anyone, including parents of the student, without the prior written consent of the student, unless disclosure is allowed under the law or under certain circumstances. Faculty/staff may access non-directory information only if they have a legitimate academic Need-To-Know.



Enrolled Student Records

DIRECTORY INFORMATION

Ordinarily, this data may be revealed by the University without student consent **unless** the student designates otherwise.

- Name
- Directory Address
- Phone Number
- Mailing Address
 - Secondary Mailing
 - Permanent Address
 - Residence Assignment
 - Room or Apartment Number
 - Campus Office Address (for Grad Students)
- Electronic Mail Address
- Specific Semesters of Registration at UTEP
- Degree(s) Awarded
 - Date(s)
 - Major(s)
 - Minor(s)
 - Field(s)
 - University Degree Honors
- Institution Attended Immediately Prior to UTEP
- ID Card Photographs

For more information please refer to the UTEP [FERPA](http://catalog.utep.edu/content.php?catoid=1&navoid=14#Student_Educational_Records) Web page
http://catalog.utep.edu/content.php?catoid=1&navoid=14#Student_Educational_Records



Disclosure of Information

- ALL external requests for disclosure of “Directory Information” must route through either:
 - **Registrar’s Office** (Students)
(915) 747-5544; OR
 - **Vice President for Business Affairs (VPBA)**
Open Records Office (Faculty/Staff/Other)
tpia@utep.edu, Fax (915) 747-5068, or Mail
<http://admin.utep.edu/Default.aspx?tabid=47537>



For More Information...

- **Information Security Office**
 - Call 747-6324
 - Email security@utep.edu
 - Visit the **ISO** websites at:
 - <http://admin.utep.edu/security>; or
 - <http://admin.utep.edu/securityawareness>
- **Office of Institutional Compliance**
 - Call 747-6478
 - Email at complianceoffice@utep.edu
 - Visit the **OIC** website at:
 - <http://admin.utep.edu/compliance>



For More Information...

- **FERPA**
<http://www2.ed.gov/policy/gen/guid/fpc/ferpa/index.html>
- **UTEP Student Educational Records (Registrar's)**
[http://catalog.utep.edu/content.php?catoid=1\\$navoid=14#Student_Educational_Records](http://catalog.utep.edu/content.php?catoid=1$navoid=14#Student_Educational_Records)
- **Payment Card Industry Data Security Standards (PCI DSS)**
https://www.pcisecuritystandards.org/security_standards/index.php
- **UTEP Information Security Policies**
<http://www.admin.utep.edu/Portals/1424/Security%20Policies.pdf>
- **Texas Public Information Act**
www.oag.state.tx.us/AG_Publications/pdfs/pia_easy.pdf
- **Texas Government Code § 552.001, et seq.**
<http://www.statutes.legis.state.tx.us/Docs/GV/htm/GV.552.htm>
- **UT System Information Resource Use and Security Policy (UTS165)**
<http://www.utsystem.edu/bor/procedures/policy/policies/uts165.pdf>
- **Gramm-Leach-Bliley Act**
<http://business.ftc.gov/privacy-and-security/gramm-leach-bliley-act>

