Basic Safety Rules for Email

Phishing & Identity Theft Scams

Phishing is an attempt to gain access to your confidential information (passwords, usernames, bank accounts, PINs, etc.) by posing as a trustworthy organization. Examples of sites often impersonated by phishers include financial institutions (your bank, PayPal), ecommerce sites (Amazon, eBay), social media sites (Facebook, Twitter) and even Whitman College. Phishers may ask you to respond by reply email, by filling out a form on a website, or by calling a phone number. Frequently, they'll claim you've won a prize or threaten you with some action, such as deletion of your account, if you do not respond.

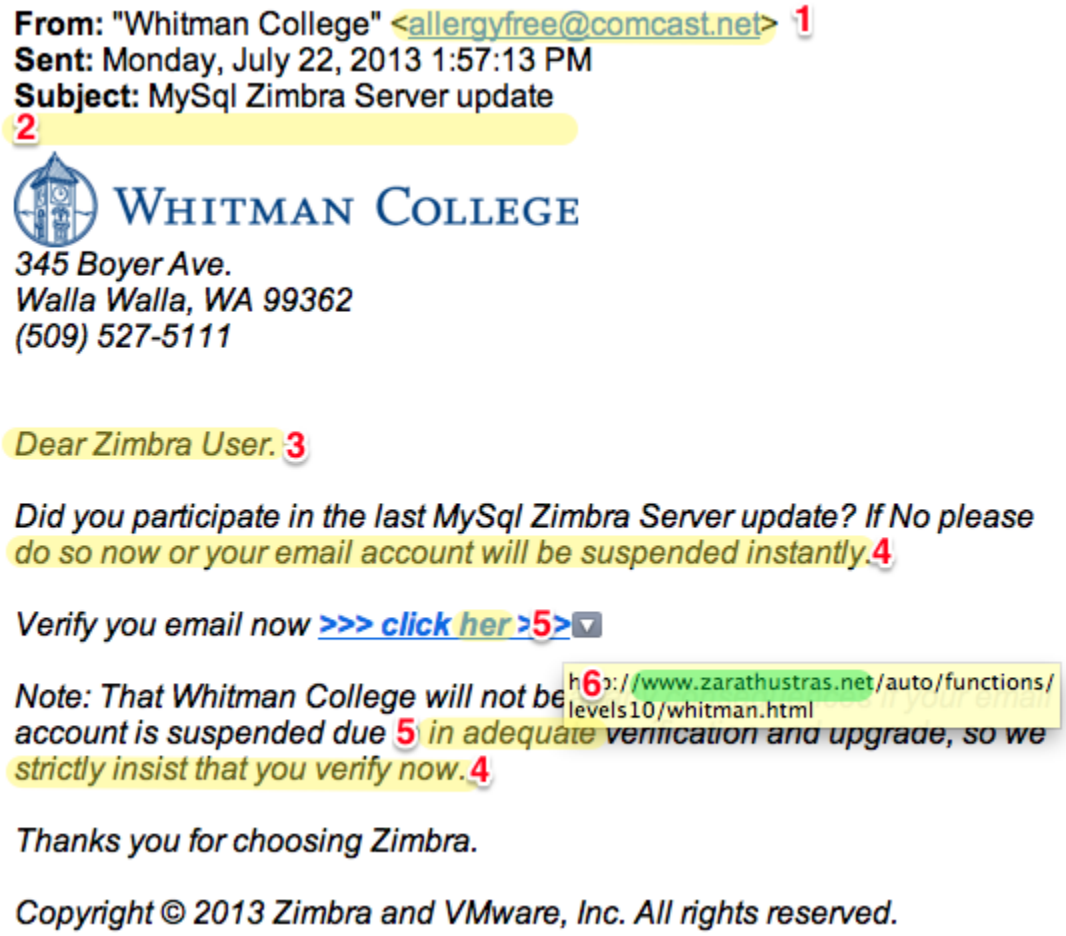
The most common form of phishing email attempts to dupe the receiver into clicking a link to a fraudulent website, where the victim is asked to enter personal information.

Other conventional ploys: "Please click to verify your account." "You have won one million dollars." "Your account will be deactivated if you don't respond within x hours."

So how do you identify phishing messages from legitimate email?

Identifying a phishing message

The following is an example of a real phishing message sent to Whitman users that is full of fraudulent email indicators. Look at the legend below the image for more information.



1. **A 'From' address that doesn't look right.** *From* addresses can be easily falsified, so take these worth a grain of salt. That said, careful inspection of the *From* properties can indicate something's up, such as the non-Whitman address listed here.
2. **'To' address shenanigans.** There are several ways the *To* address can indicate something's off:
    - It's completely missing, such as in this example.
    - Multiple recipients are listed, often with accounts that begin with the same letter of the alphabet.
    - A completely different recipient altogether.

3. **Generic greeting**. Most legitimate institutions have your information on file and will address you by name. A "Dear Valued Customer" salutation is suspect. However, phishers can mine public records and social networking sites for your personal details, so don't assume a message is safe just because it contains your name or other trivia.
4. **Threats or limited offers that create a sense of urgency or anxiety.** Fraudsters rely on your acting on impulse or in fear to override the warning signs you might have noticed, albeit subconciously. If you ever get a message like this and it looks legitimate, please contact Technology Services for verification before proceeding.
5. **Mistakes in grammar or spelling**. Real organizations do mess up, but if the message is so full of errors your elementary school teacher wouldn't accept it, it's likely a scam.
6. **Links to unrecognized or slightly misspelled sites**. Most email fraud uses malicious links as it's relatively easy to craft a fraudulent web page that looks legitimate, and criminals can install malware simply by having you visit a malicious page.

   The best way to stay safe with links in email is to ***"Hover before you click!"*** Look at the link and see if it makes sense. There are a couple of things to look for:
   a. If the mail claims to be from Whitman, but the link points to a different site, as in this example, it's probably not legitimate. You can always contact the purported sender for verification first.
   b. Variations of legitimate site names are another common strategy. Some examples would be *www.whtman.com*, *www.verify-whitman.edu*, or *www.whitmane.du*.

Phishing Precautions

- Instead of clicking email links, open a new browser window or tab and type in the address manually.
- If something seems suspicious, email the institution using a customer service email listed on its website (again, type this in by hand in a new window) to verify its authenticity.
- Heed your browser if it tells you a site may be forged.
- Never give personal information to insecure sites. Many browsers display an unbroken key or lock icon for a secure site. Click the key or lock to check the security certificate and make sure it matches the site.
- Even if you're confident a site is legitimate, test it: Enter fake information into the form before providing your genuine credentials. A phishing site will accept the false info, but the real site will give you an error.
- If you must call a customer service number from an email, never provide any personal details about your account.

General Security

Email is not a secure form of communication, as messages can be intercepted in transit.

- Avoid sending any sensitive information over email.
- If you must send a sensitive file, use a netFiles ticket. Be certain to delete the file from your netFiles account and empty your trash. You can also contact Whitman's IT Security Officer (*itso@whitman.edu*) to discuss other strategies.

Viruses

Emailed attachments can come bundled with viruses. Downloading an attachment, even one with a harmless name, can infect your computer. Only open attachments if you trust the source. Many people choose only to open attachments that they have confirmed through verbal communication with the sender.

Non-malicious spam (an oxymoron?)

Unsolicited bulk email messages can fill up your mailbox and become extremely frustrating. To avoid this predicament:

- **Don't give your email address to sites you don't trust**. Many people have an alternate email they use when buying a product from a site for the first time or signing up for a new service.
- **Don't post your email address to public places online** like message boards, comment boards, or even your personal website. Spambots crawl the web looking for these easy targets.
- **If you receive spam, don't open it or click "unsubscribe."** Spammers can use these actions to detect that your email address is active. The result: more spam. Instead, mark the message as spam in your email client and filter similar messages to the trash.

Related articles

- OUCH! - Information Security Newsletters
- Whitman College Work from Home
- Multi-Factor FAQ
- Multi-Factor Authentication - MFA
- Encryption