Don't be a victim of identity theft!

Phishing **[1] and spam emails continue to appear in campus email. Please don't reply to them or click on any links!**

Despite all our warnings, HSU faculty, staff, and students are still clicking on and/or responding to fraudulent email messages. When you do this, you are handing your HSU User Name [2] and Password over to the scammers, who then use them to generate even more fraudulent email. The more they do this, the likelier they are to hit gold - access to banking and credit card information, social security numbers, health insurance data - all of which they can sell for a lot of money.

It is VITALLY important that you keep your HSU User Name and Password safe and NEVER share it with anyone.

HSU will never ask you to provide your password, social security number, or any other personal information by email. **If in doubt, do NOT respond to suspicious email, and do NOT click on any links in suspicious emails.** Make use of the Gmail and Outlook spam and phishing reporting tools [3] and forward suspicious email to help@humboldt.edu [4].

Any of the following characteristics is a potential indicator of a fraudulent email:

- You are asked for **sensitive information** (for example, "Click here to verify your username and password")
- The message contains **spelling or grammatical errors, or strange wording** (for example, thank you, from trusted administrator)
- **The email is threatening** (for example, if you don't do this, your account will be turned off or deleted)
- The email directs you to a **slightly incorrect web address** (for example, by asking you to visit http://www.humboldt.com/account [5] instead of humboldt.edu)
- The message appears to come from an **unknown or untrusted sender** (for example, from administrator@humboldt.com [6])
- The email contains **unexpected/inaccurate content** (for example, 'you've exceeded your email quota')
- The message is **generically addressed** (for example, "Dear HSU customer")
- You are asked to **download something** (for example, "Click here to get the necessary virus [7] update file")
- **You are asked to act urgently** (for example, "You must click here immediately to avoid having your account terminated")

Questions?

If you have any questions or concerns regarding fraudulent email offers or warnings, please contact the Technology Help Desk [8] or call (707) 826-HELP (4357). You can also find more information about spam and phishing emails on the ITS website [9].

HSU staff and students are STILL falling victim to email scams. Please remember that it's not just your security, but the security of all the information you have the authority to access on HSU networks that's at risk when you respond to or click on anything in a fraudulent email. Learn more about how to avoid email scammers [10].

Related Topics

Passwords & Digital Identities [11]

Source URL: http://www2.humboldt.edu/its/dont-be-a-victim

Links:
[1] http://www2.humboldt.edu/its/glossary/5#term202
[2] http://www2.humboldt.edu/its/glossary/5#term99
[3] https://www.humboldt.edu/its/security-spam
[4] mailto:help@humboldt.edu
[5] http://www.humboldt.com/account
[6] mailto:administrator@humboldt.com
[7] http://www2.humboldt.edu/its/glossary/5#term199
[8] http://www.humboldt.edu/tech-help
[9] http://www.humboldt.edu/its/security-phishing
[10] http://www.humboldt.edu/its/dont-be-a-victim
[11] http://www2.humboldt.edu/its/category/quicklinks/passwords-digital-identities