Don't be a victim of password theft!

Don't be a victim! HSU faculty, staff, and students continue to receive and, more importantly, respond to fraudulent email messages. When you respond to a fraudulent email, your HSU User Name [1] and Password are stolen and used to generate even more fraudulent email. This increases the risk of unauthorized access to University data, and gets in the way of legitimate HSU email via external providers such as Gmail [2].

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

Humboldt State University will never ask you to provide your system password, your 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 spam and phishing [3] reporting tools and forward suspicious email to help@humboldt.edu [4].

Any of the following characteristics are potential indicators 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, do this or else your account will be turned off or deleted)
- The email directs you to **slightly incorrect web addresses** (for example, visit the HSU page by visiting: 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].

Despite all our warnings to the contrary, 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: https://www.humboldt.edu/its/dont-be-a-victim

Links:
[1] https://www.humboldt.edu/its/glossary/5#term99
[2] https://www.humboldt.edu/its/glossary/5#term195
[3] https://www.humboldt.edu/its/glossary/5#term202
[4] mailto:help@humboldt.edu
[5] http://www.humboldt.com/account
[6] mailto:administrator@humboldt.com
[7] https://www.humboldt.edu/its/glossary/5#term199
[8] http://www.humboldt.edu/tech-help
[9] https://www.humboldt.edu/its/security-phishing
[10] https://www.humboldt.edu/its/dont-be-a-victim
[11] https://www.humboldt.edu/its/category/quicklinks/passwords-digital-identities