What To Do If You Responded to a Phish

• Change your UH password immediately. If you use the same username/password combination on other sites, change those too.
• Check your email settings to make sure nothing has been enabled such as email forwarding.
• If you provided personal information such as your SSN or credit/debit card number, alert the credit bureaus, file a police report, and notify your bank.

State of Hawai‘i CPJAD
http://ag.hawaii.gov/cpja/idtheft/if-you-need-help/

Credit Bureaus
www.equifax.com
www.experian.com
www.transunion.com
www.innovis.com

Always remember that the University of Hawai‘i will not arbitrarily solicit personal information from you. You should never reply to those requests.

If you’re not sure you responded to a phish, change your password ASAP just in case.

UH InfoSec

www.hawaii.edu/infosec
infosec@hawaii.edu
www.facebook.com/uhinfosec
www.twitter.com/ITSecurityUH

IT Security Resources @ UH

Manage your UH Account and Password
www.hawaii.edu/username

Report a Phishing Attempt
www.hawaii.edu/askus/966

See the Latest Security Alerts
www.hawaii.edu/its

Need Help?

ITS Help Desk
Website: www.hawaii.edu/its
Email: help@hawaii.edu
Oahu: (808) 956-8883
Neighbor Islands: (800) 558-2669

Confused About Phishing?
Cybercriminals craft legitimate-looking email to trick you into divulging your personal information. To keep yourself from becoming a victim, remember to "SEAR the Phish."

Stop
Don’t panic and don’t be too quick to click on email links even if the message looks urgent and threatening.

Examine
Look at the email closely. Does the message look suspicious, does the link look unusual, does the request make sense?

Ask
Question the sender (if you know him/her personally). Check with the ITS Help Desk (help@hawaii.edu) to determine if the email is legitimate or not.

Report
Notify ITS if you receive any UH-related phishing emails by forwarding it to phishing@hawaii.edu

Signs of a Phishing Email
- Makes the recipient believe that their email account has been compromised or will be suspended.
- Threatens the recipient and conveys a sense of urgency with the need to respond.
- The URL of the phishing link is suspicious and the domain name does not look legitimate.

Find Out if Phishers are Already in your Account!
Using a browser, log into your Gmail account and click on the “Details” link on the right-side of the page footer to see your recent activity.

Look for sign-ins that you didn’t perform. If you see any, change your password immediately.

(Please visit hawaii.edu/askus/1587 for specific instructions.)