

Compromised Network Account Procedure

Lander University network accounts represent Lander University to the Internet community and therefore must be protected from phishing, hacking, or other fraudulent access. Failure to protect accounts from unauthorized access poses significant threats to the integrity of the Lander University network; personal information entrusted to Lander University by employees (faculty and staff), students, and other affiliates of the university; and the ability of Lander University to freely participate in Internet communications with other institutions, businesses, and individuals.

Due to the implications for Lander University if accounts are compromised, Lander University's Information Technology Services Department may disable any Lander University network account that is reasonably believed to be compromised (based on large amounts of spam being sent from the account, response to fraudulent emails asking for username and password information, propagation of virus activity, etc.). The user of the compromised account will be notified as soon as possible. Once the account owner has been made aware that the account has been compromised and agrees to take reasonable steps to resolve the problem, network privileges may be restored. If the account must be disabled after 5:00pm, on a weekend, or during a university holiday, the account may remain disabled until the resumption of normal business hours.

If you believe that your account has been compromised or have questions about this procedure, please contact the ITS Help Desk at (864) 388-8234 for assistance.