INFORMATION TECHNOLOGY
THE UNIVERSITY OF UTAH

New IT security process for compromised uNID accounts

You're receiving this email because you're subscribed to UIT's public email list.

The University of Utah's Information Security Office (ISO) has reported a sharp increase in phishing and other types of cyberattacks targeting university student accounts, which have resulted in a growing number of compromised uNID accounts.

Details

The attackers are using phishing and social engineering to gain access to users' uNID login information, including obtaining the answers to account security questions.

The ISO has implemented a new process that requires impacted users to contact their respective central help desk, verify their identities, and receive assistance to establish a secure password. Students with compromised accounts will be required to use Duo Security two-factor authentication (2FA). Employees are already required to use Duo 2FA for their uNID accounts.

The phishing attacks often impersonate U faculty, staff, students, or organizations to obtain a person's uNID and password, usually through an email asking the user to verify their account details with a link that redirects to a fake login screen. The social engineering attacks involve manipulating users into performing actions (e.g., buying gift cards) or divulging confidential information.

In addition to obtaining users' personal information, recent attackers have used a combination of phished and socially-engineered information to reset user passwords, allowing the attackers to keep using compromised accounts even after the password has been changed.

To protect accounts against phishing and other cyberattacks, **please help educate your users** so they use these IT security best practices:

- If they're not already doing so, use multifactor authentication for their university and other online accounts. **Students are encouraged to proactively begin using Duo 2FA, available at no cost, to better secure their uNID accounts.**
- If they believe they've been the victim of a phishing attempt or other cyberattack through their uNID account:
  - Forward the suspicious email as an attachment to phish@utah.edu.
  - If they opened a questionable link or answered a suspicious email, and divulged login credentials, answers to security questions, or other sensitive information, they should immediately go to CIS and change their password, then call their central IT help desk to report the attack:
    - **Main campus, 801-581-4000, option 1**
    - **University of Utah Health, 801-587-6000**

Node 4 story idea? Email us: stratcomm@it.utah.edu

it.utah.edu

NotifyIT | Follow us on Twitter | IT Services Status | IT Service Portal