Best Practice - Compromised Account Recovery

Security

If you know or even suspect your passphrase or account may have been compromised, you should immediately:

- **Notify the ITS Consulting Center of the security breach. Call 319-273-5555 immediately. The ITS Consulting Center will then notify the security office and applicable system administrators on your behalf.**
- **Change all of your UNI passphrases (see here [1]). Have them reset if necessary.**
- **Notify your supervisor as soon as possible.**
- **Work with your computer support staff to make sure your accounts are functioning properly.**

Never send your UNI passphrase via e-mail, instant message, or telephone. Do not type it into web sites except official UNI web sites. Your passphrase is not *just* for e-mail, you have a lot to lose if you type it into someone else's computer that is untrusted, not maintained properly, or infected.

Regardless of the communication method, UNI will *never* ask you for your passphrase.

Remediation Steps

Note: These are not precautions based on theoretical possibilities. All the scenarios below have occurred after accounts were compromised because individuals sent their passwords to criminals in response to fraudulent requests.

Have you sent one of your UNI passwords/passphrases through e-mail or instant message? Typed it in to an infected or untrusted computer? Typed it in to a compromised or untrusted web site? Told it to someone over the phone? If so, there are many things that need to be done besides changing your password/passphrase.

After changing your password/passphrase, you may need to verify other information accessible via your accounts have not been changed. Seek assistance from your computer support staff or the ITS Consulting Center in following these directions. It is important that these steps be followed.

Login to UNI Email [2], go to Settings, and check the information in the following fields for accuracy:

- Reply-To - Criminals may change this field so that replies people send in response to your messages will go to the criminals. This causes lost messages, compromise of sensitive communications, and information about additional UNI accounts and people criminals can use in subsequent social engineering attacks. (Via the "Accounts" tab)
- Signature - Criminals may add SPAM text and/or malicious web links to this field. This exposes all the recipients of

all your messages to SPAM and/or malicious links or could cause your messages to be thrown away as SPAM. (Via the "General" tab)

- Email forwarding - Criminals may add their e-mail address to the forwarding section so that all e-mail messages intended for you instead get sent to the criminals. This causes lost messages, compromise of sensitive communications, and information about additional UNI accounts and people criminals can use in subsequent social engineering attacks. Check your information by going to the "My Email" tab and clicking the link for "Forward email to another address." (Via the "Forwarding and POP/IMAP" tab)

Login to MyUNIverse [3] and check the following for accuracy:

- Directory Information - Criminals may alter your mailing address and phone number in the system to receive communications intended for you. Check your information by going to the "Update My Personal Information" pagelet and then clicking the link for "Update My Personal Information."

The ITS Consulting Center will notify Email and MyUNIverse administrators to check your account for evidence of tampering and unauthorized access and provide further instructions if necessary.

Login to the e-Business system [4], if applicable:

- Check all information the system allows you or someone knowing your password to change. Correct as necessary. The ITS Consulting Center will notify e-Business administrators to check your account for evidence of tampering and unauthorized access and provide further instructions if necessary.

Login to UNI's eLearning site [5], if applicable:

- Check all information the system allows you or someone knowing your password to change. Correct as necessary. The ITS Consulting Center will notify eLearning administrators to check your account for evidence of tampering and unauthorized access and provide further instructions if necessary.

Additional risks to consider:

Share rights - An attacker could make changes to your Google Drive, Google Calendar, Google Sites, or other Google services to share content with unauthroized individuals. You should verify your Google Drive, Google Calendar, and other services to make sure your content is shared as you expect it to be.

Web publishing accounts - If you have a web publishing account and someone has your password/passphrase, they may be able to change your web site to include offensive content or malicious software. Web visitors may mistake such altered content as being intentionally posted by you or the University and cause significant harm to the University's and your own image. The ITS Consulting Center will notify UNI website administrators to check your account for evidence of tampering and unauthorized access and provide further instructions if necessary.

VPN remote and wireless account - Your UNI username and password/passphrase can be used by criminals to access parts of the UNI network normally inaccessible off-campus. Depending upon your role, these may include things like Windows file servers, departmental shares, and other software and services restricted to UNI. The ITS Consulting Center will notify your computer support personal to check your account for evidence of tampering and unauthorized access and provide further instructions if necessary.

Remote Desktop Access - If you use your UNI username and passphrase to access your desktop via Microsoft Remote Desktop, Apple Remote Desktop, SSH, VNC, and similar tools, your desktop may be accessible to criminals knowing your passphrase. The ITS Consulting Center will notify your computer support personal to check your account for evidence of

tampering and unauthorized access and provide further instructions if necessary.

Encryption - Some encryption products rely on some UNI usernames and passwords/passphrases. Although not usually accessible remotely, a criminal knowing your password/passphrase will be able to decrypt your hard drive or other data you have encrypted using these types of encryption products.

Non-UNI accounts - If, contrary to recommendations, you synchronize your UNI passwords/passphrases with non-UNI services, those services will be accessible to criminals knowing your password.

Source URL: http://uni.edu/its/support/article/1053

Links:
[1] http://www.uni.edu/password/
[2] http://www.uni.edu/email/
[3] http://myuniverse.uni.edu
[4] https://ebiz.uni.edu
[5] http://www.uni.edu/elearning