Cyber Security Month: Week 2

Don’t Fall for Phishing Scams

Security is everyone’s responsibility. Please diligently watch for phishing and scam emails. Current circulating scams involve unsolicited job offers and requesting your contact information while impersonating someone you may know. They frequently request you share your phone number or contact information, and/or purchase gift cards. Scammers often pose as leaders in the University to try to fool you into fulfilling their requests. Our NKU leaders would not make such requests.

Please be sure to verify a suspicious email with the sender via another form of communication. If you think any email may be malicious or if you are unsure, please forward it to abuse@nku.edu.

Watch our security video to avoid phishing attacks.

Keep your Software Updated

Updating software is a critical practice in today’s digital age. It’s not just about getting the latest features or a sleeker interface; it’s about security, stability, and efficiency. Software updates often contain patches for vulnerabilities that cybercriminals can exploit, safeguarding your data and privacy. They also enhance performance, fix bugs, and improve compatibility with other applications. By regularly updating your software, you not only ensure a smoother user experience but also protect NKU and yourself from potential threats in an ever-evolving digital landscape. In essence, updating software isn’t just a choice; it’s a vital responsibility for anyone using technology in the modern world.
What to do if Your Account has been Hacked

If you suspect that your account has been hacked, immediate action is crucial to minimize potential damage and regain control:

1. **Change Your Password**: Start by changing your password to something strong and unique. Use a combination of letters, numbers, and special characters.

2. **Enable Multi Factor Authentication (MFA)**: If available, enable MFA for an extra layer of security. This requires a second form of verification, such as a one-time code sent to your phone, to log in.

3. **Check for Unauthorized Activity**: Review your account activity to identify any unauthorized actions or changes. This includes checking your recent login history and any altered settings.

4. **Log Out of All Sessions**: Most services provide an option to log out of all active sessions. This will immediately disconnect the hacker from your account.

5. **Monitor Your Accounts**: Keep a close eye on your accounts for any unusual activity and consider changing your passwords regularly.

6. **Update Other Accounts**: If you used the same password for multiple accounts, change those passwords as well to prevent further breaches.

7. **Educate Yourself**: Learn about common hacking techniques and how to spot phishing attempts to avoid falling victim again in the future.

Remember that acting swiftly is crucial when dealing with a hacked account. The sooner you take these steps, the better your chances of minimizing damage and regaining control of your digital identity. If you have any doubts or concerns, please contact the [IT Help Desk](https://it.nku.edu/).

https://it.nku.edu/
Check our website for the latest system alerts and news.
Follow updates on Twitter [@NKUCIO](https://twitter.com/NKUCIO)