Keep your payroll information safe

Cyber Criminals target online payroll information for employees within higher education. They target you through a variety of phishing scams designed to capture your login username and password. Once the hacker has your credentials, they sign into the Employee Self Service portal to change banking information and reroute payroll deposits.

All public universities have seen an attempt such as this made many times. Hackers will try to get you to click on a malicious link via a phishing attempt to compromise your username and password. Once hackers have your information, they can act on it right away or they can sit on it for months. Regardless, their next step is to go into your email and reroute anything that says payroll or direct deposit to your trash or junk mail folder. These criminals have gone so far as to create mail filters to reroute or delete emails based on Payroll employee's names and email addresses so you don't receive any notifications of changes made to direct deposit. Once the notification emails are rerouted, the hackers now have access to reroute the direct deposit to another bank account or prepaid card. You will not be aware of this until payday when your paycheck is not deposited into your bank account.

Payroll and IT Security have been working together diligently to stay one-step ahead of this threat vector. Payroll will be using a number of factors to determine the validity of all direct deposit requests and may reach out to certain individuals based on the mode and method by which the user requests a direct deposit change.

What can employees do to safeguard their information?

Do not open or click on links in emails that look suspicious. Hold your cursor over links in emails or check the email address to verify where it's really coming from. Be aware that these criminals are getting very good and some of these emails look completely legitimate.

If you do accidentally click on a link or suspect you may have been a victim of a phishing scam **change your FlashLine password immediately from a different machine, if possible.** If you need assistance doing this you can contact the helpdesk (330-672-4357) and they will walk you through it.

When a change is made to your direct deposit, you will be sent emails notifying you of the change. The email will go to both your Kent State and your alternate email *if one is available*. It is recommended that you have an alternate email set up for this reason.

Change your FlashLine password regularly; just because it isn't a requirement doesn`t mean it's not a good idea. Contact the helpdesk for any questions related to this article. For direct deposit assistance please contact payroll at payroll@kent.edu or 330-672-8640.