NOTICE: The Information Security Office would like to make you aware of some new threats to your personal information.

FBI Warns of University Employee Payroll Scam

Some university employees have received fraudulent emails indicating a change in their human resources status. The email contains a link directing the employee to login to their human resources website to identify this change. The website provided appears very similar to the legitimate site. Once the employee enters his/her login information, the scammer captures that information, uses it to login to the employee’s legitimate human resources account and changes the employee’s direct deposit information. This redirects the employee’s paycheck to the bank account of a scammer.

Consequences of this scam:

- The employee’s paycheck can be stolen.
- The money may not be returned in full to the employee.
- The scammers can take the employee’s log-in credentials and attempt to log into other accounts that belong to the employee.

Tips on how to protect yourself from this scam:

- Look for poor use of the English language in emails such as incorrect grammar, capitalization and verb tenses. Many of the scammers who send these messages are not native English speakers.
- Roll your cursor over the links in the email and look for inconsistencies. If the url displayed is not the website the email claims to direct you to, the link could direct you to a fraudulent site.
- Never provide credentials of any sort via email.
- When receiving an email that requires you to login to an account, always access your account by entering the web address in your web browser or by clicking the link in your ‘favorites’ or ‘bookmarks’ menu. Never access the site from a link provided in the email.
- Contact the WUSTL Information Security Office at infosec@wustl.edu if you receive suspicious email.

FBI Warns of Fictitious ‘Work-from-home’ Scam Targeting University Students

College students across the United States are being targeted to participate in work-from-home scams. Students are receiving emails to their school accounts recruiting them for payroll and/or human resources positions with fictitious companies. The position simply requires the student to provide his/her bank account number to receive a deposit and requires the student to transfer a portion of the funds to another bank account.
The compensation the student receives is derived of funds stolen by cyber criminals. In receiving and transferring these funds to a second account, the student unknowingly becomes involved in perpetuating the scam. This is a crime which could lead to the deactivation of the student’s bank account and/or federal charges.

Consequences of participating in the scam:

- The student’s bank account will be identified by law enforcement as being involved in the fraud.
- The victim employee has his/her pay stolen by the scammers utilizing the student’s bank account.
- The student could be arrested and prosecuted in federal court. A criminal record will stay with the student for the rest of his/her life and will have to be divulged on future job applications, which could prevent the student from being hired.
- The student’s bank account may be closed due to fraudulent activity and a report could be filed by the bank.
- This could adversely affect the student’s credit record.

Tips on how to protect yourself from this scam:

- Never accept a job that requires the depositing of funds into your account and wiring them to different accounts.
- Look for poor use of the English language in emails such as incorrect grammar, capitalization, and verb tenses. Many of the scammers who send these messages are not native English speakers.
- Never provide credentials of any kind such as bank account information, login names, passwords or any other identifying information in response to a recruitment email.
- Forward these emails to the WUSTL Information Security Office at infosec@wustl.edu and tell your friends to be on the lookout for the scam.

**SPAMBot Attack on Campus**

Finally, faculty and staff have reported receiving emails requesting that they click to open a zipped PDF document. These files infect the computer with malware and begin sending SPAM messages with malware to infect more computers. This malware slows down school email and provides the attackers with opportunities to steal user accounts and add additional malware to steal other information on the computer.

Tips on how to protect yourself from this malware:

- Do not click on attachments that you are not expecting.
- Roll your cursor over the links in the email and look for inconsistencies. If the url displayed is not the website the email claims to direct you to, the link could direct you to a fraudulent site.
- Never provide credentials of any sort via email.
When receiving an email that requires you to login to an account, always access your account by entering the web address in your web browser or by clicking the link in your ‘favorites’ or ‘bookmarks’ menu. Never access the site from a link provided in the email.

Contact the WUSTL Information Security Office at infosec@wustl.edu if you receive suspicious email.