Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

May 05, 2017

Alert Number

I-050517-PSA

Questions regarding this PSA should be directed to your local **FBI Field Office.**

Local Field Office Locations: **www.fbi.gov/contact-us/field**

RECENT FRAUD SCHEMES TARGETING UNIVERSITIES AND THEIR STUDENTS

A recent analysis of over 500 reports from victims of fraud who were targeted because they were U.S. universities or their students identified several key trends that have been observed across the country since at least July 2016. Scammers who continue to target these groups are primarily motivated by financial gain. While some appear to be extremely organized and methodical, others are less sophisticated, but nevertheless have proven to be successful in their efforts.

Financial loss to higher education institutions has approached one million dollars from a recent single occurrence. Students have sustained financial losses of several thousand dollars each from a common scam.

The FBI is highlighting the following popular scams to raise awareness, and to provide tips on how the public can protect itself from becoming a victim.

Vendor Bank Account Update Scam

Many universities are frequently engaged in large construction projects which require regular electronic payments of at least several hundred thousand dollars. It is relatively easy for a criminal to identify the construction companies involved in these projects and use social engineering and e-mail spoofing to commit this type of fraud. As a result of the nature and large size of these payments to a construction company, losses are significant.

How the scam works:

- The scammer, posing as an established vendor, sends an e-mail to the university's accounting office with bank account changes to be used for future payments.
- Typically, it is an individual purporting to be from a construction company with which the university has an existing business relationship.
- The scammer often spoofs the actual e-mail address of the company with a similar domain. For example, if the actual domain is

abcbuilders.com, the scammer might register and use abc-builders.com to send the e-mail.
- The university sends their next payment to the scammer's bank account, and the money is often unrecoverable by the time the university realizes they have been the victim of fraud.

Tips on how to protect yourself from this scam:

- To verify the request is legitimate, always contact an individual at the known and previously used telephone number of the company requesting the change to their bank account information.
- Establish procedures at your university that include a means to authenticate requests to update any existing vendor financial information.
- Look closely at the domain the e-mail address is being sent from to confirm that it matches the actual known domain of the vendor. Be aware that e-mail spoofing may be used, so do not rely on this method alone.
- Forward suspicious e-mails to the university's IT department and report it to the FBI's Internet Crime Complaint Center at www.IC3.gov.

Fake "Education Tax" Scam

The IRS and the FBI will never contact an individual by telephone regarding taxes owed or to request an immediate payment of past due taxes. All communications between the IRS and an individual are sent via U.S. mail. The IRS will never threaten to immediately send the police to arrest an individual for not paying taxes. In addition, the IRS will never require you to pay via a prepaid debit card or gift card. Unsuspecting college students have lost a significant portion of their savings to this crime.

How the scam works:

- A scammer will contact a college student via telephone claiming to be from the IRS or FBI.
- The caller ID is spoofed and displays the local FBI field office telephone number.

- The scammer tells the victim they must remain on the phone the entire time and not hang up. At times this has lasted several hours.
- The scammer will demand immediate payment of a fake "education tax" that has not been paid.
- The student is told that if they do not pay their taxes that day, the caller will send the local police to arrest the student.
- The scammer often requests payment via a major US-based retail chain store's gift card or a popular tax preparation company gift card, which allows for the anonymous transfer of funds to the scammer.
- The scammer nearly always will tell the victim which stores to go to and how much money to put on each gift card.
- Once the gift card is purchased, the caller requests the account number on the card.
- The scammer often states that this is not enough money, and instructs the victim to purchase additional gift cards at specific locations.
- The prepaid gift cards are immediately used by the scammer, and the withdrawn funds are unrecoverable.

Tips on how to protect yourself from this scam:

If you receive a call from someone claiming to be from the IRS or FBI demanding immediate payment for taxes:

- Immediately hang-up and do not provide any information.
- Contact the U.S. Treasury Inspector General for Tax Administration (TIGTA) at 1-800-366-4484 to report the call or complete the form at https://www.treasury.gov/tigta/contact_report_scam.shtml
- If you have been a victim of this scam or any other Internet-related scam, you may file a complaint with the FBI's Internet Crime Complaint Center at www.IC3.gov and notify your campus police.

Phishing Scheme Involving Requests for W-2 Tax Information

For the second year in a row, the FBI has observed a trend involving a phishing scheme targeting payroll departments and human resources professionals related to requests for W-2 tax information. This scam often emerges around the end of January, and has been successful at

compromising personally identifiable information (PII), which includes full name, date of birth, social security number, and salary information. The stolen PII can be used to commit other fraud including filing fraudulent tax returns to collect refunds.

How the scam works:

- The scammer poses as a high-level executive (University President, CFO, or Treasurer) and sends an e-mail to the payroll department requesting W-2 information for all employees.
- The scammer may use the actual name of the executive; however, the scammer may rely on outdated information, and mistakenly pose as an executive who is no longer affiliated with the university.
- The scammer may request this information be compiled in a PDF document or Excel Spreadsheet.
- There are varying levels of sophistication used in e-mail spoofing.
    - For example, if the real domain is AbcUniversity.edu, the scammer might use a similar fake domain such as AbcUniversityedu.com or AbcUniversity.com
    - Scammers also used a fake payroll related domain.

Tips on how to protect yourself from this scam:

- Even if the e-mail appears to come from an executive you know, always contact that individual at their known telephone number to verify their request is legitimate.
- Look closely at the domain the e-mail address is being sent from to confirm it matches the actual known domain of the university. Be aware that e-mail spoofing may be used, so do not rely on this method alone.
- Look at the "reply to" section of the e-mail headers to confirm it matches the sender's e-mail. This has proven to be one way to identify a spoofed e-mail address when the domain of the "reply to" e-mail address is not the university's domain.
- Forward suspicious e-mails to the university's IT department and report it to the FBI's Internet Crime Complaint Center at www.IC3.gov

Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

Phishing Scheme Involving Payroll Fraud

This scam involves a more sophisticated cyber actor who employs a tradecraft that is well planned. The actor obtains access to the payroll system and alters direct deposit information to commit payroll fraud and receives money via a pre-paid credit card.

How the scam works:

- The scammer purporting to be a university executive uses e-mail spoofing to send an e-mail with a PDF attachment to staff.
- Upon opening the PDF, the user is prompted to enter log-in credentials.
- The scammer uses the credentials to log into a payroll processing system.
- The scammer then changes the direct deposit information for that university employee to have their pay electronically sent to a pre-paid credit card.
- The scammer creates rules in the university employee's e-mail account that immediately forwards incoming e-mails containing words such as "phishing, direct deposit, payroll, bank, etc." to the deleted folder so the employee does not get alerted to the criminal activity.

Tips on how to protect yourself from this scam:

- Do not open attachments or click on links from unknown individuals.
- Confirm the "reply to" section of the e-mail header matches the sender's e-mail. This has proven to be one way to identify a spoofed e-mail address when the domain of the "reply to" e-mail address is not the university's domain.
- Never enter your log-in credentials when opening an attachment or clicking a link in an e-mail.
- Forward suspicious e-mails to the university's IT department and report it to the FBI's Internet Crime Complaint Center at www.IC3.gov
- Universities should establish appropriate policies requiring verification of payroll account changes to confirm the changes are authorized.

The IC3 produced a PSA in January 2017 titled "Employment Scam Targeting College Students Remains Prevalent," which mentioned another type of scam. This PSA can be viewed at https://www.ic3.gov/media/2017/170118.aspx.

The IC3 produced a PSA in May 2014 titled "Cyber-Related Scams Targeting Universities, Employees, and Students," which mentioned similar scams. This PSA can be viewed at https://www.ic3.gov/media/2014/140505.aspx.

Federal Bureau of Investigation, Cyber Division

Public Service Announcement