Compromised Employee Accounts FAQ

> This FAQ is directed towards supervisors of employees, but is also relevant in most regards to the employees themselves whose accounts are compromised.

What does it mean when an employee’s account is considered “compromised?”

An account is considered compromised when there is evidence that someone other than the user has had access to the account or if there is a high degree of probability that a user’s login name and password have been exposed. This use can range from sending spam/phishing emails to a hacker actually being able to log into a person’s Banner account and steal or change sensitive information such as payroll direct deposit information. Because of the high risk such compromises pose, CIS has created a policy whereby suspect accounts are marked as “compromised.” Once compromised, the credentials are no longer valid and the user must contact CIS for remediation. More details on this process are explained below.

SPU email administrators monitor various notification lists and public sites to detect if and when SPU email accounts are compromised. Once we have a high degree of certainty that a compromise has occurred, we mark the SPU account as “compromised,” thereby suspending the validity of the account in question.

How was the account compromised?

In most cases, we don't know for certain. In fact, CIS often knows less about how the account was compromised than the account owner. Sometimes, the user has responded to a phishing message or clicked a suspicious link. Most commonly, account owners have used the same password across multiple accounts (for instance, SPU, Facebook, and Google, etc.) and one of those systems is breached.

Why would there be no notification of compromised provided to the SPU email account in question?

Automatic emails are sent to all the employee's email addresses on record whenever we mark any account as compromised; this includes the SPU email address as well as any other email addresses we have on file. However, often the malicious user will delete any email notifications sent to the SPU email address, perhaps before the employee sees it. If no additional email addresses are on file, the employee may see no notification; For this reason, we strongly encourage all users to have an additional email on file. To add one, go to Update External Email Address in Banner Self-Service.

What data was compromised?

CIS will work with employees and supervisors if it is determined that sensitive data may have been compromised. There are two main subsets of data that may be at risk:

1. Office365 (including Email, Sharepoint, OneDrive, etc.) - We can determine whether a malicious user logged in to Office 365, but may not be able to verify what they viewed or edited. Typically, hackers use compromised SPU email accounts to send phishing messages targeted at other SPU users. As part of this, mailbox rules might be created to hide the suspicious activity from the unsuspecting employee. We rely on O365 email alerts to advise us when compromised accounts are being used for phishing.
2. Other Data systems (including Banner, Raiser's Edge, Canvas, etc.) - We can determine whether a malicious user logged in to our Single Sign-On portal, but may not be able to determine quickly all applications that were accessed. Specifically with Banner, we can identify what pages were loaded (in both Self-Service and Banner Admin). Typical targets here include pay stub and direct deposit information. If there are specific data systems you are concerned about, we can attempt to identify or verify what access may have occurred.

Was sensitive data compromised?

If Office365 resources were accessed, the extent of data at risk is limited to what is present in email history, OneDrive, etc., as well as any third party accounts for which the SPU email address would provide access (for instance, if access to the email allows resetting the password to an online banking account).

If Banner was accessed, then pay stub and W2 information may have been exposed, including the SSN, as well as academic information (like grades) for which the faculty/staff member has access.

Will SPU provide credit monitoring?

Unless the compromised account occurs due to an institutional data breach where SPU is at fault, the University will not provide credit monitoring or other follow-up investigation. As noted in the Computer Acceptable Use policy, "Users must take appropriate and reasonable measures to protect the integrity, exclusiveness, and confidentiality of individual resources and account credentials."

CIS assistance only includes marking the account as compromised (removing access), initial notification, verification of whether sensitive institutional data was breached, regulatory obligations were violated, and restoration of access.