APPSIAN

SOLUTION BRIEF

Safeguarding PeopleSoft Against Direct Deposit Theft

A guide to mitigating payroll diversion attacks and keeping ERP data safe

Abstract

On September 18, 2018, the FBI issued an alert[1] stating that "cybercriminals are targeting the online payroll accounts of employees in a variety of industries." These attacks have since been popularized as payroll diversion scams and direct deposit theft. In most successful attacks, hackers imitate a legitimate sender's email account and send phishing emails to employees, prompting them to enter their payroll/ERP credentials on a fake login page. Once the employees' credentials are captured, hackers will login to alter direct deposit information and divert paychecks to a bank account under their own control.

Payroll diversion attacks are accomplished using compromised credentials and employers typically only learn of the breach once employees begin reporting their missing paychecks. What's worse is that hackers can stay within the system undetected long enough to change the info back, leaving organizations with no clue of what happened. While banking information is the primary target in these attacks, hackers will often explore other parts of the application – potentially exposing sensitive information.

The breach of personally identifiable information (PII) also makes employers liable for penalties under data privacy regulations such as GDPR. Regulatory liabilities further increase when organizations miss breach notification deadlines due to a lack of evidence. In totality, the price, time, and efforts associated with detection, remediation, and reporting of payroll diversion attacks can be significantly high. Rooted in phishing attacks, the success of this scam relies on social engineering to exploit human error. Unfortunately, no security controls can be implemented to control the human factor, and multiple security leaders[2] have agreed that human beings are still the weakest link in an organization's security strategy. The challenge is to build security features that can mitigate identity-based threats, before and after credentials are compromised.

In this solution brief we will discuss security challenges associated with handling payroll diversion in PeopleSoft. The document focuses on how user awareness, contextual access controls, and fine-grained data security can help organizations mitigate payroll diversion.

Some notable payroll diversion events[5] from the recent past:

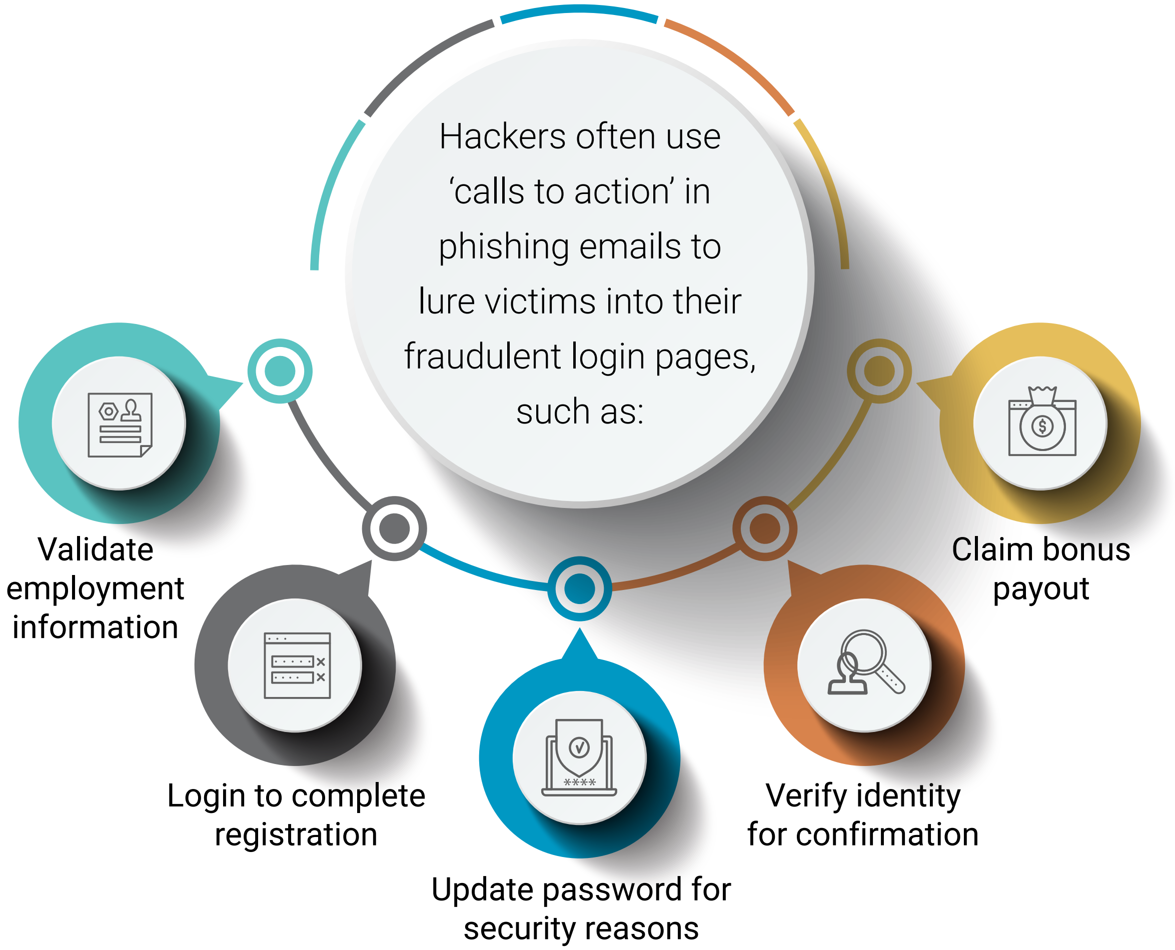
1. In March 2019, 200 employees at the City of Tallahassee did not receive their paychecks after hackers diverted $500,000 of payroll. While the underlying reason of the attack is under investigation, city officials and security experts speculate that it was caused by a phishing attack on the city's 3rd party managed payroll system.

2. Hackers are expanding their tactics and targeting not only employees but HR officials as well, effectively convincing them to change direct deposit information on behalf of the employees. While security features cannot dodge such tactics, user awareness and strict self-service protocols can prevent them from being successful.

3. The University of Pittsburgh warned users of a 'payroll notification scam' where hackers were attempting to collect employee usernames and passwords by mimicking the University's login page.

4. Atlanta Public Schools had $56,459 stolen in a payroll diversion scam and discovered several unauthorized changes in direct deposit information of employees. It was also reported that confidential data of all 6,000 of the district's employees may have been compromised in the attack.

5. Several employees at Denver Public Schools in Colorado fell for a phishing email which resulted in scammers diverting over $40,000 of pay. Hackers used a phishing email so convincing that despite perimeter security features and user awareness initiatives, 30+ users clicked on it.


Hackers often use 'calls to action' in phishing emails to lure victims into their fraudulent login pages, such as:
Validate employment information
Login to complete registration
Update password for security reasons
Verify identity for confirmation
Claim bonus payout

Challenges

Why Are Hackers Successful?

According to the Verizon Data Breach Investigations Report[3], 30% of phishing messages get opened by targeted users, and 12% of those users click on the malicious attachment or link.

Most successful payroll diversion attacks stem from hackers who exploit human error to their advantage. These hackers use advanced phishing techniques to prey on unsuspecting employees and lure them into providing valid login credentials to access sensitive information. Despite investment in user awareness and training programs, employees continue falling for phishing emails. In fact, the frequency of successful attacks has significantly increased in the past couple of years. According to the 2019 State of the Phish report[4], credential compromise rose 70% from 2017-2018, and it has increased 280% since 2016.

The Password Problem

The password once used to be the beacon of security, so much so that legacy ERP applications like PeopleSoft relied only on a username and password for authentication. However, depending on a single set of credentials is no longer effective!

Conditioning users to enter their password every time they access their account grooms them for exploitation. As password-based login becomes a routine, almost a mindless action, users become susceptible to the fraudulent login pages that hackers are using to phish credentials – and victims may only realize what has happened after the damage is done.

Mobile & Remote Access Brings New Challenges

Many organizations are choosing to expand access to PeopleSoft self-service modules to the public internet. The flexibility of remote access allows employees to perform tasks from anywhere, on any device – delivering increased productivity and efficiency. However, it also greatly expands an organization's attack surface. If employees are granted full access outside a secure corporate network, hackers who gain access via phished valid credentials will also have no limitations on what they can access remotely – allowing incidents like payroll diversion to happen.

Limited Visibility Hinders Detection and Response Efforts

Combating payroll diversion requires granular visibility into PeopleSoft activity. Since hackers are using phished credentials to gain access, details around what was viewed inside PeopleSoft and information on a user's device, IP address, and location must be recorded. Without this information, it is extremely difficult to decipher valid access from compromised access.

Unfortunately, PeopleSoft's native logging capabilities cannot provide this crucial information. Designed in an era before the proliferation of user-centric threats, PeopleSoft logging was originally built to provide data used for testing and troubleshooting. This means that logs are bulky, system-focused, and impractical to scale at the coverage necessary to record user activity without significant performance implications. Due to these reasons, most organizations must limit logging to only record user login and logout activity.

Solution

A multi-pronged approach is required to mitigate the impacts of payroll diversion. Organizations must address the "human factor" and focus on reducing the success phishing attacks by training users to recognize, avoid and report suspicious emails and fake login pages. Additionally, security enhancements on data protection can help minimize repercussions of compromised credentials. Organizations must also strive to achieve actionable intelligence to fast-track threat detection, exploration, reporting and response.

Reduce the Rate of Credential Compromise

Educate Users About Phishing and Payroll Diversion Scams

User awareness is a key to thwarting phishing attacks. Continuous education and training programs can help reduce the risk of employees falling for payroll diversion scams. Organizations must invest time and resources on training their employees to:

- ✓ Never share credentials or personal information via email. Follow up on requests via chat, phone call or in person
- ✓ Be cautious of illegitimate password reset requests, employment validation requests, or other unexpected CTAs requiring your credentials
- ✓ Click on a sender's name to verify whether the 'from' email address is legitimate and review URLs by hovering their cursor over hyperlinks before clicking
- ✓ Forward suspicious emails to HR and IT departments and alert the appropriate contacts if they believe their credentials have been compromised

Eliminate Manual Logins with Single Sign-On for PeopleSoft

Using a Single Sign-On solution means that users will no longer be conditioned to manually enter their credentials each time they login. By removing this action, fraudulent phishing pages that request a manual login will seem out of place and stand a higher chance of being caught by your users.

Appsian's PeopleSoft SSO Connector brings native SAML compatibility into PeopleSoft and enables organizations to easily configure Single Sign-On integrated with their respective Identity Provider. With an SSO solution installed, features like embedded links allow users to access specific modules without requiring a password once a login attempt has been authenticated by an identity provider.

Mitigate the Risk of Compromised Access

There's no fool proof way to combat phishing - every organization will have users who fall prey despite the best preventive measures. Once a hacker obtains valid credentials, application-level security measures that can mitigate malicious access are an organization's last line of defense.

Appsian Security Platform (ASP) is purpose-built for PeopleSoft and enhances security controls at the field, page, and component levels within the application. By combining contextual user and data information with fine-grained security controls, ASP ensures that sensitive data and transactions stay protected, even when credentials are compromised.

Secure User Identity with Multi-Factor Authentication

Adding a second form of authentication to PeopleSoft means that even if a user's ID and password is compromised, access can be still blocked. While traditional 3rd party MFA solutions can be integrated at PeopleSoft login (with custom development), enforcing arbitrary MFA challenges at every login can hinder usability and cause pushback from end-users.

ASP enables organizations to contextually enforce MFA challenges at login and inside the application (for example, at the banking information page). Tying in contextual information, such as location, device, or data sensitivity, allows organizations to enforce MFA only where needed, in turn matching security with risk and improving usability.

Protect Remote Access with Location-Based Security

ASP enhances PeopleSoft with contextual access controls that provide the protection necessary in today's dynamic business environment. Adding flexibility to access control policies, ASP allows organizations to dynamically change privileges based on the context of access. For example, organizations can block remote access to high risk transactions (i.e. changing bank account info) or enforce additional security measures (such as MFA or data masking) when access is outside of a trusted network. ASP's location-based security can significantly reduce the risk of remote access and enables organizations to better align to the principal of least privilege.

Gain Direct Visibility into PeopleSoft with User Activity Logging

ASP records user activity on a granular level, enabling organizations to identify suspicious access and follow up on user-activity around banking information. Combined with fine-grained security features, ASP generates detailed logs enriched with contextual information such as the location of access, what was viewed, when, by whom, device, IP address and more. By providing a full audit trail of user activity, ASP's logs allow security teams know exactly what was accessed when a user's credentials were compromised. These logs also help organizations fast-track incident response and stay prepared for regulatory or internal reporting.

Deploy Real-Time Analytics to Expedite Detection and Response

Detailed PeopleSoft user activity logs are fundamental to security audits. Without this information most organizations would be flying blind. However, manual analysis must still be performed, and this takes time.

ASP's Real-Time Analytics extension allows customers to visualize detailed user activity logs on SIEM dashboards to gain actionable intelligence. Data visualizations highlight noteworthy patterns and trends, enabling customers to quickly identify suspicious activity. Drill down capabilities allow security teams to further investigate suspicious transactions and view a complete audit trail of a user's activity. By reducing the time required to detect and investigate security incidents, ASP improves PeopleSoft incident response capabilities and alleviates the pressure of looming breach notification deadlines.

Summary

Payroll diversion scams can cause direct and unrecoverable monetary damages. The repercussions of attacks can escalate to regulatory non-compliance and associated penalties if remediation and reporting efforts are slow. Well-strategized security layers combined with user awareness can be instrumental in preventing payroll diversion. However, organizations must always be prepared to mitigate imminent threats.
With continuous user-activity monitoring and deep visibility into payroll activity, organizations can achieve the oversight needed to respond to threats effectively.

About Appsian's Security Platform

Appsian Security Platform (ASP) allows PeopleSoft customers to enhance their security posture by enabling fine-grained data protection and contextually aware security features. ASP is the only solution of its kind that natively integrates into the PeopleSoft webserver without requiring additional hardware or impacting the underlying PeopleCode and future updates.

By layering identity verification and contextual access control capabilities, ASP can help organizations prevent damaging payroll diversion attacks. Furthermore, granular logging and deep activity monitoring simplifies incident response efforts. The best part - ASP is cost effective and has a shorter implementation timeline in comparison to the alternative of multiple custom integration projects.

References

[1] https://www.ic3.gov/media/2018/180918.aspx

[2] https://securityintelligence.com/how-to-build-a-corporate-culture-of-cyber-awareness/

[3] https://www.ictsecuritymagazine.com/wp-content/uploads/2017-Data-Breach-Investigations-Report.pdf

[4] https://www.proofpoint.com/sites/default/files/pfpt-us-tr-state-of-the-phish-2019.pdf

5 - Payroll diversion events:

https://www.tallahassee.com/story/news/2019/04/05/almost-500-k-swiped-city-tallahassee-payroll-hack/3379242002/

https://www.vadesecure.com/en/vade-secure-uncovers-ongoing-direct-deposit-spear-phishing-attacks/

https://www.technology.pitt.edu/news-and-alerts/phishing-alert-pittsburgh-payroll-notification-scam-mimics-pitt-passport-login-page

https://www.ajc.com/news/local-education/atlanta-schools-says-confidential-data-for-all-employees-potentially-exposed/gGg8UGVudZmQH6b9Ao9geI/

https://kdvr.com/2017/04/05/phishing-scam-diverts-more-than-40k-from-denver-public-schools/

APPSIAN

8111 Lyndon B Johnson Fwy. Dallas, TX 75251

☎ +1 (469) 906-2100

✉ info@appsian.com