Always Designing for People®

Date: March 14, 2023
From: ADP Global Security Organization
Subject: Social Engineering and Phishing Campaigns: Bank Closure Scams

There is a heightened threat of social engineering attempts as a result of recent banking events. Some clients have received fraudulent emails appearing to come from companies that have been impacted by recent bank closures. These emails may request your credentials, personal identifiable information, and updates to bank information "to ensure smooth continuation of payment services".

**How to Report a Phishing Email to ADP**

Be alert for this fraudulent email and follow the instructions below if you receive any suspicious email:

- Do not click on any links or open any attachments within the message.
- Forward the email as an attachment to abuse@adp.com, then delete it.
- If you clicked any link or opened an attachment in the email, immediately contact your IT support.

**How to Protect Yourself**

It is critical that you and your employees be proactive and alert. By educating your employees on safe email practices, including how to recognize and report suspicious emails, you can help mitigate the threat of phishing scams.

- For Payroll Administrators:
  - Be cautious of requests for bank account changes that originate via email, as they may appear to be from an employee, but might in fact be fraudulent; therefore, it is critical to verify the validity of the email and employee's identity before taking additional action.
  - If you receive a phone call from a known employee for a bank account change, do not give out any information or process any changes until you validate the caller's identity through another method (i.e., in person, by calling the known contact number, instant message, etc.,).

- For Employees:
  - As stated on their website, the FDIC will not send unsolicited email notifications to claim/unlock/suspend your account. The FDIC, however, will encourage you to correspond with them via the FDIC Claims Portal, a secure web portal.
  - If you receive a phone call asking you to change your bank account, do not give out any information or process any changes until you validate the caller's identity through another method (i.e., in person, by calling the known contact number, instant message, etc.,).
  - If you received a notification of a change that you did not authorize, contact your payroll department immediately.

The Global Security Organization continues to actively monitor this situation. Clients are encouraged to visit our website at www.adp.com/trust to learn more about how ADP protects data, and how clients can help protect themselves. Protecting our clients and their data from malicious activity is a top priority for ADP.

**Additional Resources**

If you or your employees have been impacted by the recent bank closures and are experiencing difficulties or have questions, we are here to help. For more information, please visit our Resource Hub here.