CIBM BANK

CENTRAL ILLINOIS BANK

MARINE BANK
Milwaukee | Indianapolis

Member FDIC

IMPORTANT SECURITY ALERT
for Business Clients

Our data processing partner, Jack Henry, indicates that there is increased activity with a malware screen takeover that is targeting token users. This particular malware variant will prompt a user to input account and/or token data, which then results in another screen prompt indicating that the user will be unable to access the account for 24-hours while maintenance is performed. This allows the fraudster to take over the session and commit fraud while the user is detained on the fake "maintenance" screen.

A similar variant of the malware has been identified where the end user receives a pop up asking for several pieces of personal information including a phone number. The customer inputs the data and then receives a phone call immediately from a caller claiming to be a bank employee letting them know the system will be down for 24-hours which then allows the fraudster to access the account while on the phone with the user.

Initial data is also showing the following characteristics about this malware:

- The malware is designed to collect data such as watermarks and FI logos to make the false screens appear legitimate.

- The fraud attack takes place with IPs that are not the same as the customer. CIBM Bank offers an optional solution to prevent this type of fraud by restricting IPs through our Trusted IP option. This security feature prevents fraudsters from accessing Online Banking accounts when the IP address does not match the IPs on file for the actual customer. Learn more about this feature by contacting CIBM Bank customer service at 877-925-3030 for more information regarding the Trusted IP option.

- Signs to watch for include experiencing difficulty logging in *or* closing sessions – particularly token users.

<u>Users who are infected should immediately conduct an anti-virus scan.</u>

At CIBM Bank we alert you in advance via message(s) at our Online Banking Login Screen regarding upcoming system maintenance. Also, feel free to contact your support team before entering account or token information on new or unfamiliar screens.

As a reminder, tokens are one component in an overall security posture which your company should have in place. Please see our brochure regarding security tips "Protecting Yourself from Online Banking Fraud".

Thank you.

CIBM BANK