**EXECUTIVE SUMMARY:**

The following branches were tested as part of this engagement:

* Oak Lawn Branch: 9640 South Pulaski Road, Oak Lawn, IL 60453
* Des Plaines Branch: 249 South River Road, Des Plaines, IL 60016
* Winfield Branch: 27W460A Chicago Ave, Winfield, IL 60190
* Naperville Branch & Headquarters: 1151 East Warrenville Road, Naperville, IL 60563-9339

The engagement consisted of a physical test of predefined branch locations for Healthcare Associates' Credit Union. These tests were designed to examine the capability of an unanticipated individual attempting to access restricted areas, documents, and systems. The methodology of the test consisted of two phases arranged to test employee adherence to the organization’s security policies. During the first phase, the TraceSecurity Information Security Analyst attempted to provide minimal identification and use coercive techniques to gain unauthorized entry into restricted areas of the facilities. The second phase of the test determined if onsite personnel follow appropriate security procedures when an outside individual enters sensitive areas of the facility.

During this engagement the analyst presented themselves as a Field Inspector for ADApt Consulting that was assigned the organization’s address for an alleged violation of ADA compliance to state or federal regulators. Under this cover story the analyst explained that all areas, public and private, would need to be inspected without prior announcement, to prevent the organization from tampering or fixing areas that would otherwise be a violation. A business card and company ID badge were presented by the analysts as two forms of false identity during the engagement. The analyst was also equipped with a clipboard containing ADApt Consulting stickers, a false checklist/form, and a tape measure.

Healthcare Associates' Credit Union (HACU) employee compliance with policies showed significant gaps during the onsite exams for allowing unauthorized or scheduled visits to the locations, identity verification, and documentation of the visits.

An itemized list of the gaps found during this exam are listed below with more details regarding the findings and recommendations for correcting these can be found within the report.

* Incomplete Physical Security Zones: The physical zones within the organization allowed unauthorized access through unlocked doors from the stairwell. Departments that are designed to require access badges prior to entry were not fully locked and could be accessed through alternate areas such as hallways and stairwells.
* Shadowing Techniques Allowed: Employees permitted unauthorized persons to access secure areas of the facility through a technique called shadowing; which allows an unauthorized person to hold a previously locked door open after an authorized person has passed through the entryway.
* Unscheduled and Unauthorized Visits Permitted: The presence of individuals within and around the financial institution that have no banking needs should only be permitted to remain in the facility or on the facilities' private grounds with prior authorization.
* No Identity Verification Procedures Detected: Proof of identity should be verified and cross examined with a government issued ID. Company identification should be collaborated and researched prior to granting visitors authorization.
* No Visitor Documentation or Logging: Authorized visitors should be documented with a logbook that collects entry and exit times, purpose of visit, responsible party at the organizations, company represented, and areas accessed during the visit. A visitor badge should also be dawned by the individual to clearly identify and classify the visitor to other members of the organization.
* No Visitor Escort Policy Enforced: Visitors to the organization that have been granted access should be monitored and escorted by authorized personnel at all times.
* Sensitive Information Left Unattended: Computer screens and printed material should be protected at all times from unauthorized access. Any office, computer, or document that contains sensitive information should be locked or stored away when left unattended by the responsible party.
* Sensitive Information Disclosure: Details about the employees, facility, or other information disclosed to unauthorized visitors can aid future attacks to the organization with tactics formed around the information voluntarily disclosed during conversations and eavesdropping.
* Written notes and photographs taken by visitors should only be allowed with extreme caution. Detailed information about the security of the facility, number of personnel within the building, surveillance equipment, and exits are just a few items that a malicious person may want to document during reconnaissance phases of an attack. Once notes and observation examples are permitted by the organization, detailed copies of the information should be retained with the visitor logs and inspected by the organization.

**LOCATION DETAILS:**

**Location Summary:**

The analyst presented themselves as a Field Inspector for ADApt Consulting that was assigned the organization’s address for an alleged violation of ADA compliance to state or federal regulators. Under this cover story the analyst explained that all areas, public and private, would need to be inspected without prior announcement, to prevent the organization from tampering or fixing areas that would otherwise be a violation. A business card and company ID badge were presented by the analysts as two forms of false identity during the engagement. The analyst was also equipped with a clipboard containing ADApt Consulting stickers, a false checklist/form, and a tape measure.

[details] The analyst was allowed to inspect the location without prior authorization. Although the analyst was escorted throughout the inspection, the identity of the analyst was not verified with government issued credentials nor was the information provided inspected or verified. At no time did the analyst witness a log entry of the visit and was not asked to sign a logbook or wear a visitor badge or other identification.

**ID:**

A self-printed business card and company ID badge was all that was provided during the visit. The identification provided was not cross checked with government issues credentials or inspected for authenticity.

Proof of identity should be verified and cross examined with a government issued ID. Company identification should be collaborated and researched prior to granting visitors authorization to ensure the individual(s) is legitimate.

TraceSecurity recommends implementing a vendor/visitor management policy with documentation and escort procedures. Vendor/visitor management policies should include authorized personnel listings and individual verification of each representative of the organization prior to onsite meetings, inspections, or visits.

**LOGBOOK:**

The analyst was not asked to fill out a visitor log book nor did the analyst witness a logbook or system being filled out.

Authorized visitors should be documented with a logbook that collects entry and exit times, purpose of visit, responsible party at the organizations, company represented, and areas accessed during the visit. A visitor badge should also be dawned by the individual to clearly identify and classify the visitor to other members of the organization.

TraceSecurity recommends implementing a centralized logging system to track the entry/exit, purpose, organization represented, point of contact during for the escort, and areas accessed during the visit.

**PRIOR AUTHORIZATION:**

The analyst was permitted to conduct a false examination of the facility without prior authorization. Although the analyst was escorted at all times during the visit, information was provided for the location of sensitive information and intimate details about the facility were available to the analyst that can be used by malicious parties to plan a detailed attack such as exits, camera coverage, utility rooms, server rooms, etc.

The presence of individuals within and around the financial institution that have no banking needs should only be permitted to remain in the facility or on the facilities' private grounds with prior authorization.

TraceSecurity recommends classifying different visitor types and asking the individuals to wear a badge to clearly identify them to the employees of the organization.

**VISITOR BADGE:**

The analyst was not classified as a visitor nor asked to wear identification during the visits that would clearly notify the other employees that the analyst was authorized or had been granted access to the facility.

A visitor badge should also be dawned by the individual to clearly identify and classify the visitor to other members of the organization. Visitor badges can limit the range of an intruder within the organization by allowing employees to immediately mark whether a stranger has been authorized or not. While escorting third parties/vendors can mitigate many risks, this adds an additional layer of security to help prevent a third party/vendor from leaving their escort unauthorized or an attacker from convincing employees that s/he is authorized to be in a non-public area.

TraceSecurity recommends requiring all third parties/vendors to wear a visitor's badge when accessing non-public areas of the facility.

**ESCORT POLICY:**

The analyst was not monitored and escorted at all times while accessing non-public areas of the organization. Once the branch manager was authorized by upper management to allow the inspection, the manager did not appear to be following any escort policies or procedures during the inspection.

Allowing an individual to travel unescorted could allow a social engineer access to workstations, documentation left on printers and desks, mail, and other sensitive equipment and/or documentation. Additional controls should be in place to detect and prevent this sort of malicious activity.

TraceSecurity recommends training users on the dangers of an unescorted visitor in the building, and how to either approach the individual(s) for verification or alert a member of management team.

**Supervision: SENSITIVE INFORMATION:**

The analyst was able to access unoccupied areas of the branch without supervision that contained sensitive information. The analyst was left alone with the information long enough to take photographs of documents and/or computers without detection.

Computer screens and printed material should be protected at all times from unauthorized access. Any office, computer, or document that contains sensitive information should be locked or stored away when left unattended by the responsible party.

TraceSecurity recommends that a clean desk policy is enforced and tested to ensure that no sensitive information is left unattended in an insecure location.

**Voluntary SENSITIVE INFORMATION:**

During the unauthorized visit the analyst was provided with sensitive information about the location, members, customers, or other critical infrastructure items and locations that would be used by a real attacker to gather information and customize future attacks to increase successful access to disrupt services or gain direct access to personal identifiable information (PII).

Locations of critical equipment or equipment storing PII, record storage areas, and security controls should be guarded and remain private during any visitor engagement. Although a visitor may be escorted during their engagement, the intent could be to gather intelligence about the facility, location of services, information, and otherwise critical systems. Exposing unauthorized users to the location of this equipment can lead to tailored attacks with more success.

TraceSecurity recommends that all visitors be approved by key personnel prior to any engagement. Prior authorization procedures should include verification of employment, validity of the inspection claims, and proper scheduling with key personnel to conduct any inspections of the facilities maintained by the organization’s private public and public areas. Key personnel should be trained appropriately to identify suspicious activity and reduce exposure to sensitive information, areas, and other critical information or systems and their location.

**FORMS NOTES AND SIGNATURES:**

Throughout the visit the analyst collected notes and details about the visit that did not related to the inspection described as part of the cover story. The notes collected were directly related to the location of cameras, alarm key-pads, the presence of security guards, and locations revealed during the visit that contain critical or sensitive information.

Social engineering attacks are designed to be conducted under any radars or suspicious activity to prevent the engagement from being discovered as an investigative event to learn key pieces of information about the targeted organization. In a series of low-profile visits the malicious party can expand the attack vectors over time until the information is provided or exposed in a way that would compromise the organization disrupt the organizations productivity. This type of information could be collected with photographs, videos, or simple notes taken by the visitor.

TraceSecurity recommends that all artifacts collected during visits by third-party providers be inspected and copied prior to the individuals or groups exiting the facility. This will allow the organization’s representatives to further inspect the visit for suspicious activity and document more details of the visit’s logbook entry.