The Evangeline
BANK AND TRUST COMPANY

Account Takeover

Account Takeover is a cybercrime where cybercriminals obtain access to an online account (banking, payment app, email, social media, etc.) to fraudulently transact, steal sensitive client data or hold data for extortion or ransom. Criminals takeover accounts to gain access to confidential and personally identifiable information and to financial accounts with the goal of financial gain.

Compromised information can be sold on the dark web to other criminals leading to identity theft, held for extortion and ransom, scaring victims into sending demanded payment, used to impersonate victims to gain access to additional accounts or to portray to be someone else in an effort to build a connection with someone and then convince the victim to send money. Access to financial accounts/information allows criminals to transfer funds to money mule accounts, make unauthorized purchases/payments or redirect electronic payments.

How can my information fall into the wrong hands?

Credentials can be compromised in several ways. Attackers may trick individuals into disclosing login information, install malware on devices where credentials are stored or used, or rely on automated attacks that test stolen username and password combinations.

Once criminals gain access, they can hijack online sessions or email accounts, monitor user activity, review account history, collect sensitive information, obtain credentials and change personal details or passwords. These changes can lock legitimate users out of their accounts, which is why this crime is known as account takeover.

Phishing and Social Engineering. Criminals use deceptive emails, phone calls, text messages or websites to persuade victims to reveal credentials. They may also encourage victims to click malicious links or open infected attachments or images that install malware on their devices.

Malware and Zero-Click Exploits. Some attacks do not require the victim to click a link or take any action. In a zero-click attack, criminals send specially crafted data—such as a hidden code in an image, PDF, missed-call notification or audio message—to a built-in app. This can silently install spyware or malware that hijacks sessions and captures information.

Credential Stuffing and Brute-Force Attacks. Criminals use automated tools to test username and password combinations, often using credentials exposed in prior data breaches. If people reuse passwords across accounts, one compromised password can give attackers access to multiple services.

How to Protect Yourself and Your Business

In today's digital environment, cybersecurity is more critical than ever. Threats continue to evolve, putting businesses at risk of data breaches, monetary loss and reputational damage. To help protect your business, we recommend at a minimum, following these essential practices:

Employ Strong Passwords

Utilize strong, unique passwords or passphrases for all your online accounts. This means using special characters, upper-case and lower-case letters, as well as numbers.

Keep Passwords Confidential

Never share your passwords, PINs or 2FA codes with anyone, regardless of their requests. Save passwords in a secure environment.

Enforce Regular Password Changes

Configure parameters that force users to change passwords on regular intervals.

Enforce Account Lockout for Invalid Login Attempts

User accounts should be configured to lock after 3 invalid login attempts. Unlocking the account for programs allowing access to sensitive information should require administrative action.

Disable saved passwords in browsers

Credential keeper software is available and can be safer if properly configured to enforce MFA via authenticator app/physical token with a timeout of 4 hours or less. Storing passwords in your browser can be risky because if your device is compromised by malware or accessed by someone else, your saved credentials can be easily exposed. Additionally, browser-based password storage may lack the stronger encryption and security protections offered by dedicated password managers, making your accounts more vulnerable to hacking.

Enable Two-Factor Authentication (2FA)

Whenever possible, activate two-factor authentication (aka multi-factor authentication or MFA) for accounts containing sensitive or financial information, such as banking and trading accounts. This is also advised for social media accounts. An authenticator app or physical/FIDO token, rather than phone or email, are recommended for enhanced security. Do not circumvent MFA for example, by selecting "remember this device", by sharing OTPs (One-Time Passcodes) or leaving the FIDO tokens deployed.

Unique Login Credentials

Use distinct login IDs and passwords for each online account to enhance security. Never use an account such as Facebook or Google to log into other accounts.

User Access Restrictions

Remove unnecessary access to applications, especially privileged access and review access authority regularly.

Enable Network/System Access Restrictions

Restrict access to applications outside of business hours. It is also important to limit access to the network and systems, to authorized devices and only from trusted IP addresses.

Practice Safe Email/Text Message Handling- Recognize Phishing Emails/Text Messages

Handle every message with caution by verifying the sender, avoiding suspicious links or attachments and reporting anything unusual before taking action. Train yourself and your team to recognize phishing emails and text messages. Do not open suspicious attachments or click questionable links. Traditional warning signs—such as blurry graphics, misspellings and poor grammar—still apply, but phishing attempts are becoming harder to detect. Ignore unexpected attachments or links, especially from unknown senders. See the "Email Authentication Protocol" section below for more information.

Exchange Sensitive Information Securely

Do not send sensitive information by email unless it is encrypted. Use a secure file-sharing platform as an alternative when sharing this type of information.

Email Filtering

Use a reputable email filtering service to auto encrypt outgoing email containing sensitive information. Deploy software to scan email for malicious content, to quarantine and report accordingly.

Configure Firewall

Utilize a network firewall content filtering service to restrict internet browsing to business purpose needs only. Enable local firewalls such as Defender for Microsoft.

Install and Update Anti-Malware and EDR Software

Install reputable anti-malware software on your internet-connected devices and ensure it is actively running and stays up to date. Turn on auto-updates if possible and monitor status on a regular basis.

Apply Software Patches and Updates

Promptly apply critical security patches and updates released by software vendors. This holds true for all your devices, including IoT items (any device that connects to the internet such as smart thermostats, point of sale terminals, security cameras). If your older devices are no longer supported, consider getting newer ones.

Regular Data Backups

Implement regular data backups and store them on a separate device or location from your primary computer or device.

Avoid using public wi-fi access.

Using public Wi-Fi is risky because unsecured networks make it easier for hackers to intercept your data, potentially exposing sensitive information like passwords or financial details. Cybercriminals can also create fake hotspots to trick users into connecting and stealing their information. As an alternative, use a virtual private network (VPN) to encrypt your connection or rely on your mobile data/hotspot, which is generally more secure than public Wi-Fi.

Enforce Dual Control

Enforce dual control, using system functionality available for WIRE and ACH transactions, particularly for outgoing credits.

Regularly Monitor Financial Activity

Monitor accounts daily for unauthorized activity. It is important to notify the bank immediately upon discovery. Items must be returned the day following settlement day.

Utilize Positive Pay with Payee Name Verification for Checks

This service is offered by the bank and can aid in detecting altered/fictitious checks in a timely manner.

Data Storage

Whether stored electronically or in paper format, sensitive information should be kept securely with restricted access. Review permissions that allow access to electronic data. Destroy paper and other media using methods that prevent the data from being reconstructed.

Internet Use and Online Security

Risks of Unauthorized Web Surfing

Unauthorized web surfing can expose our network to several risks, including:

- Malware and Viruses: Visiting unsecured or malicious websites can lead to malware or viruses being downloaded onto our systems.
- Phishing Attacks: Web surfing increases the risk of falling victim to phishing sites that mimic legitimate websites to steal personal or bank-related information, including credentials.
- Accessing non-work-related sites increases the risk of data breaches, compromising sensitive customer and bank information.

Report unusual/suspicious activity

It is important to report incidents or suspected incidents immediately so that damage can be effectively contained. Develop internal procedures that define incident reporting protocol.

Incorporate information security awareness training

Continuously educate yourself about the latest scams and their indicators. Free resources are available to assist such as The Federal Trade Commission (https://www.ftc.gov/) and Stickley on Security.

What is Business Email Compromise (BEC)?

BEC is a type of cybercrime where attackers gain access to a business email account and imitate the owner's identity to defraud the company, its employees, customers or partners. These scams can result in significant financial losses and compromise sensitive information. Once bad actors access your email account, they will have access to all historical and current email communication. When possible, avoid sharing sensitive data via unsecured email. For example, internal documents could be shared on a file server or shared drive with proper access restrictions. Secure file-sharing platforms are also an option.

Recognizing BEC Threats

- Unexpected Requests: Be wary of emails requesting urgent financial transactions, sensitive information or other unusual actions.
- Email Addresses: Check the sender's email address carefully for any slight variations that might indicate it is fraudulent. Even when you can validate the email address is a known email address, you should still use caution.
- Often, hackers will make a request imposing a sense of urgency. Stop and use caution prior to responding to any request being made via email or phone.

Email Authentication Protocol

To protect against BEC, it is important to adhere to the following protocols:

- Always verify the source before clicking on links, attachments or images. They seem usual but may contain malware.
- Do not forward the email without first verifying its legitimacy.
- Confirm the request via a separate communication channel, such as a phone call or direct face-to-face verification. Do not email the sender to verify the legitimacy of the email and do not call the phone numbers listed in the email unless you verify that it is a known, trusted number. Otherwise, you may be communicating with the hacker.
- Examine Email Headers: Review the email headers for discrepancies in the sender's address and the email routing information.
- Report Suspicious Emails: If you receive an email that appears suspicious, do not respond or click on any links. Report it immediately to your supervisor.
- Check the sender's email address carefully for any slight variations that might indicate it is fraudulent. Even when you can validate the email address, you should still use caution. Many trusted affiliates such as attorneys, title companies, vendors, etc. have all been compromised, making you an easier target. For example, the hacker sifts through the compromised email and may use AI to impersonate the users' writing style, create rules to redirect certain emails to folders so that the compromised user is unaware and then sends a phishing or malicious email to a trusting affiliate.
- Contact your IT department or manager if you question an email's authenticity. Notify IT immediately if you believe you responded to a malicious request; acting quickly improves the chances of containing and remediating the threat.

Share Your Knowledge-Awareness is Key!

It is important that we remain vigilant and inform our co-workers, our community, our customers, our friends, our families and our business partners of the threats we are seeing and how to circumvent them.