COGENT academy

CYBER SECURITY
best practices for businesses

IDENTITY THEFT

Identity theft occurs when someone uses your personal information such as your name, social security number or credit card number without your permission.

Skilled thieves obtain information in a variety of ways:

- **Dumpster Diving:** Locating personal information from bills and bank statements you discard
- **Skimming:** Stealing your debit or credit card information using a storage device
- **Phishing:** Pretending to be a financial institution or company by sending spam or pop-up messages to get your personal information
- **Changing your address:** Diverting your bills to another location using a change of address form
- **Information compromise:** Information is retrieved from data stored on medical records or other materials
- **Stealing:** Stealing your wallet, mail, checks, or pre-approved credit offers

CYBERATTACKS

A cyberattack is any intentional effort to steal, expose, alter, disable, or destroy data, applications, or other assets through unauthorized access to a network, computer system or digital device.

PHISHING

Is a way of attempting to acquire sensitive information such as usernames, passwords, and financial details by masquerading as a trustworthy source.

- The term alludes to “baiting” with the goal that potential victims will “bite”
- Typically carried out by e-mail spoofing, instant messaging, and or by phone solicitation.

SPEAR PHISING

is a type of cyberattack that is more specialized and uniquely crafted to target specific individuals (often high-profile individuals or companies).

QUISHING

is a type of cybersecurity threat in which attackers create QR codes to redirect victims into visiting or downloading malicious content.

SMISHING

Smishing or SMS phishing is a type of cybersecurity threat in which attackers redirect victims into visiting or downloading malicious content via SMS texts.

COGENT academy

What to do if your identity is stolen:

- **Place a Fraud Alert on your Credit Reports:** Fraud alerts prevent an identity thief from opening additional accounts.
  - **Equifax** @ 1-888-Equifax or https://www.equifax.com
  - **Experian** @ 1-888-Experian or https://www.experian.com
  - **TransUnion** @ 1-800-916-8800 or https://www.transunion.com
- **Consider a Credit Freeze:** You should contact each credit bureau and set up a password. This will provide the ability to "Thaw" your credit whenever you need to have a credit check performed.
- **Contact Financial Institutions:** Close existing accounts that have been tampered with or new accounts that have been opened fraudulently.
- **Update Passwords:** Change the password for any online accounts that may have been compromised.
- **Contact IRS:** If the compromise involved tax-related documents.
  - Call the Identity Protection Specialized Unit (IPSU): 1-800-908-4490
  - File form 14039 (IRS Identity Theft Affidavit)
    - https://www.irs.gov/pub/irs-pdf/f14039.pdf
    - The IRS will issue you a PIN to use to verify your identity
- **File a Complaint with the Federal Trade Commission (FTC):** Use the online complaint form or call the hotline. The printed Identity Theft Complaint along with a police report entitles you to certain protections.
  - 1-877-438-4338 or https://www.identitytheft.gov/#/
- **Police Report:** Call the police and ask if you can file the report in person or over the phone/internet. Ensure you receive a copy of the police report or a signature on your complaint for your records. This is helpful when disputing fraudulent accounts and debts caused by fraud.

Tips to Safeguard Your Online Security:

Install Antivirus Software and Keep It Updated:

- Antivirus software protects against various types of malware, including viruses, ransomware, and trojan horses. Regularly update your antivirus to stay protected.

Explore the Security Tools You Install:

- Understand the security features of the software you use, including firewalls, privacy settings, and encryption options.

Use Unique Passwords for Every Login:

- Use complex passwords and consider using a password manager to store them.

Use Multi-Factor Authentication (MFA):

- Enable MFA wherever possible. It adds an extra layer of security.

Use Passcodes Even When They Are Optional:

- Set passcodes or PINs for your devices, even if they are not mandatory.

Pay With Your Smartphone:

- When making online purchases, consider using mobile payment apps or services. They often provide additional security features like tokenization.

For Business:

- Consider a dedicated PC when accessing online banking accounts
- Limit employee access to sensitive data and information
- Uninstall software no longer in use
- Deploy software patches in a timely manner to prevent zero-day vulnerabilities

Cogent Fraud Products to Protect

ACH Positive Pay is an online fraud mitigation service which allows you to manage ACH debits and credits posting to your business account via filters and blocks.

ACH Transaction Filters: Simply specify which ACH debit entries should be allowed to post. You can specify the originator of the transaction and even determine a dollar limit. This prevents unauthorized transactions while allowing certain transactions to occur as expected based on the parameters you have selected.

ACH Transaction Block: This can prevent unauthorized electronic transactions from occurring on your account. You may add, modify, or delete authorization records using Cogent Connection, our Online Banking service in a real-time environment.

Check Positive Pay: Positive Pay provides daily protection against losses due to fraudulent check payments and the cashing of unauthorized checks presented at a Cogent Banking Center.