Banker's Bulletin

pages.paychex.com/BankPartnerResources

Cybersecurity Tips for Your Business Clients

Cybersecurity can be defined as the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks, unauthorized access, or criminal use. IT experts agree that employees are often the weakest link in the fight against cybercrime. They often make critical mistakes because they lack the knowledge and training to recognize warning signs or avoid improper behavior while working online.

Here's a list of tips to aid in cybersecurity training and greatly enhance the security of your business data:

Cybersecurity Do's

- ✓ Use strong passwords and security questions and remember to regularly change them.
- ✓ Use good internet browsing practices.
- ✓ Keep software up to date, including latest anti-spyware and anti-virus software that secures computers, phones, and tablets.
- ✓ Enable authentication tools (e.g., authentication apps, multi-factor authentication, and more).
- ✓ Enable operating system's firewall, which can prevent outsiders from accessing data on a private network.
- ✓ Limit access to Personal Identifiable Information (PII) and Protected Health Information (PHI). Only employees whose job responsibilities explicitly require access to PII (e.g., Social Security number, bank account number) and PHI (e.g., health records, other medical information) should be granted it.

Cybersecurity Don'ts

- x Don't download software from the internet or click on internet links that launch websites or web ads.
- x Don't respond to emails, open email attachments, or click links embedded in emails that include typos, spelling errors, incorrect grammar, or pop-up windows.
- x Beware of suspicious subject lines and "urgent" calls to action.
- x Don't enter personal or financial information into web forms that don't come from a trusted source.
- x Don't respond to the IRS by email or social media. The IRS does not initiate contact with taxpayers by email, social media, or even by phone. Any contact in this manner is a scam.

Make Sure Your Business Clients are Protected from a Cyberattack

Your clients' current business insurance coverage might not include the range of expenses incurred by many types of cyberattacks — from interruption of business operations and the need for customer notifications to comprehensive security upgrades and the effort required to restore a company's damaged brand. For these reasons, consider cyber liability insurance as part of a broader cybersecurity plan in tandem with regular business insurance and employment liability policies.

An effective cybersecurity policy can help secure business interruption protection and cover legal fees incurred by judgments or settlements. Contact your Paychex rep to learn more about cyber liability coverage.

PAYCHEX®