Huntington Bank

Strong data privacy is good business.

Staying mindful of security helps protect what you've built. These practical tips can make it easier to keep your business safe without slowing you down.

Strengthen account security

- Use strong, unique passwords for each business account. Encourage your team to do the same.
- Turn on multi-factor authentication (MFA) wherever possible. It adds a second layer of defense.
- Limit access to sensitive systems and data. Only give access to those who need it.

Protect customer & employee data

- Collect only what's necessary and store it securely.
- Avoid open spreadsheets or unsecured files for private info. Use password-protected systems.
- Know where your data lives: cloud platforms, local files, or third-party tools.
- Dispose of data properly. Shred paper documents and fully delete digital files when no longer needed.

Keep devices & systems updated

- Install software updates promptly. They often fix security gaps.
- Use trusted security software on all devices connected to your network.
- Back up your data regularly and store backups securely. It helps you bounce back fast if something goes wrong.

Train & empower your team

- **Share the tips on the back of this page with your team. It's designed for you to make copies!**
- Talk about common scams.
- Help your team spot red flags like phishing emails disguised as invoices or vendor messages.
- Always be cautious of urgent requests from someone pretending to be the owner or executive.
- Be aware of tech support scams asking for access to systems or payment info.
- Encourage a "pause and verify" mindset. If something feels off, employees should be comfortable speaking up.
- Keep training simple and repeat it often to keep security top of mind.

Vet Your Vendors

- Ask questions before sharing data. Do they encrypt info? What's their breach response plan?
- Review contracts and policies. Look for clear privacy and security standards.
- Check in regularly to make sure they're meeting expectations.

SECURITY AWARENESS

Huntington Bank

Security starts with you!

Recognize fraud attempts and secure sensitive data

Fraudsters use calls, texts, emails, and social media to trick you. Here are five signs that something is not right.

1. Pressure to act fast

Slow down when you hear things like “We need payment now or your account will be closed.” Urgency is a scammer’s favorite tool. Always verify.

2. Requests for account info

No reputable company will ask for your password, PIN, or security codes out of the blue.

3. Unfamiliar numbers or links

If you weren’t expecting the message, don’t recognize the sender or the link looks odd, don’t click. Go straight to the official site or app.

4. Too good to be true

Unexpected refunds or payments due? Vendor deals that require upfront payment? Surprise giveaways asking for company info? These are all red flags.

5. Something feels off

Trust your gut. If a message sounds strange or out of character, stop and check before you respond. Staying calm and cautious is your first line of defense.

Learn More: Visit huntington.com/Security

Smart security habits at work

Protect your credentials
Use strong, unique passwords for work accounts and never share them. Enable multi-factor authentication (MFA) when available.

Protect physical documents
Don’t leave sensitive papers on desks or in unlocked drawers. Shred documents when they’re no longer needed.

Watch for unexpected messages
Pause before clicking links or opening attachments. If an email or text looks unusual or urgent, verify before acting.

Secure digital devices
Lock screens when stepping away, even for a minute. It keeps sensitive information secure.

Use secure connections
Avoid public Wi-Fi for work tasks.

Report issues quickly
If you see something odd (like a strange email or system glitch) tell your manager right away. Fast action matters.