

PINNACLE BANK

Tips to Ensure Hardware Security & Protect Your Business Data



Hardware security is necessary to ensure that data remains safe from malicious attacks.

Any type of hardware, from outdated computers to modern devices, may be at risk.

One way to mitigate these risks is for businesses to follow security best practices.

Below are some tips on hardware security that you can implement to ensure your business' data is secure.



Educate

Bad actors will always try to exploit the “human factor” when it comes to security. No matter how strong your business’ security practices are, they can be easily undone by uninformed employees or contractors.

It is essential to educate your staff about the importance of hardware security.

- Educate your employees on why hardware security is essential. Remember - It's not just about protecting your business' data; it's also about protecting your customers' data and conserving your business' reputation.
- Explain the basics of hardware security, such as proper password management and the importance of physical security, like locking up company devices when they're not in use, or ensuring devices are running on the latest system releases and security updates.
- Educate your employees on security procedures, such as reporting suspicious emails that can harm their devices.



Implement

As businesses implement a hybrid or work from home model, and as phishing and financial scam attempts are on the rise, it is more important than ever to implement physical security procedures.

- Ensure all hardware is kept in a secure location, especially when not in use.
- Limit access to hardware to authorized personnel only.
- Use dual control or multi-factor authentication (MFA) when making changes to data and hardware to avoid tampering
- Consider implementing MFA or VPN for any employees accessing your network while offsite



Document

When devices are onboarded properly, they are configured in line with your business' security standards. Old devices can also be a liability if they're not properly retired.

Ensure that your business' onboarding and termination or device disposal procedures are well documented.

- Have an intake/onboarding process - Create a process to inventory and secure every new device as it's purchased and deployed to staff.
- Have a disposal process – When a device is retired ensure that there is a decommissioning process in place. Wipe data from the device and remove it from your network.
- Have a process to report losses & harmful activity – Keep the inventory you've collected up to date, especially as soon as losses or harm to the device occurs.
- Have a process in place for employees to report suspicious activity, and loss of a device - The faster it is reported, the faster security teams can respond.

To learn more about how to protect you and your accounts click on:

[Online Banking Fraud Prevention Best Practices](#)

Contact us right away if there's a problem!

If you believe you have been the victim of a fraud scheme, detected illegitimate activity on your account, or something just doesn't seem right — contact us immediately.

We will work with you to review your transactions to understand the extent of the issue.

Pinnacle Bank

(888) 485-7050



[Get in Touch](#)

PINNACLE BANK