You Are At Risk!

Fraudsters Target Small Businesses.

BY STACY DUNN | RCB BANK INFORMATION SECURITY

Information is as good as gold.

If you think your business is too small to be a victim of data loss, think again.

Cybercriminals find small to medium-sized businesses to be more accessible targets.

While physical securities are a concern (leaving documents lying around or not shredding personal paperwork), the majority of incidents tend to be more hands off.

Hackers like to infiltrate businesses with social engineering tactics:

- Phishing & vishing
- Customer account compromise
- Vendor management intrusion

The National Institute of Standards and Technology offers a framework to help businesses protect their work spaces. Each business has unique risks and will require tailored security measures.

Preventive measures:

- Limit employee access to sensitive data.
- Use strong passwords that expire.
- Use multi-factor authentication.
- Train staff on information security.
- Reduce risk with effective policies and procedures.
- Encrypt all data, especially email and mobile devices.
- Use reliable endpoint protection, firewall and email filtering.
- Update and patch systems regularly.
- Protect all facets of your business, e.g., websites and vendor access.

Your network is only as strong as your weakest user.

Hackers are one step ahead in trying to steal information. Take steps to not become their next victim.

Information security training is a must-have in today's environment. **Invite RCB Bank's Information Technology and Business Services teams to speak about cybersecurity at your workplace.** Call 918-342-7379 to schedule an appointment. Learn more at RCBbank.com/security.

Invest in yourself.

RCBbank.com/GetFit
855-BANK-RCB

Opinions expressed above are the personal opinions of the author and meant for generic illustration purposes only.

Common Cyber Attacks

Phishing Emails: Hacker persuades the user to click on a link or provide the user's credentials, installing malware.

System Misconfiguration: Hacker takes advantage of outdated software, unnecessary services, incorrect configuration or factory settings to access files.

Injection Vulnerabilities: Hacker uses flaws in production environments that affect program coding, possibly hijacking the system.

Man-in-the-Middle Attacks: Hacker intercepts data between two points and alters the communication between those parties, impersonating one or both parties.