SPRINGS VALLEY'S CYBERSECURITY BEST PRACTICES

Make your passwords complex.

Create long passwords or passphrases using a mix of upper/lowercase letters, numbers, and symbols. Passphrases are easier to remember and harder to crack. Example: SVBTLovesTheirCommunity!2025

Routinely update your devices.

Regularly update phones, computers, laptops, and routers to protect against new threats.

Back up your data.

Frequently back up the date on all computers and phones used at home or work.

Don't grant online banking access to unknown individuals.

Scammers often pose as help desk staff or bank employees. If something feels suspicious, call us and ask for Mitch in IT/InfoSec.

Install an antivirus software on all devices.

Every device on any network should have an antivirus software running and performing daily scans for protection.

Use eMail security to reduce spam and phishing.

Use eMail filters and policies to reduce, potentially hazardous emails, and stay up to date on current phishing trends and always practice safe eMail habits.

Research any AI tools before using them.

Not all AI programs are secure—never share personal or proprietary data.

Control physical access to all devices on your network.

Keep equipment locked up and use key fobs, MFA, or other security measures to prevent unauthorized entry.

Be mindful of social media sharing.

Limit personal details, get permission before posting about others, and remember—criminals use social media to gather information.

***Loyal to you, your family,
and your future.***

springsvalley
BANK & TRUST COMPANY

svbt.bank | **800.843.4947** | *Since 1902*

Member FDIC EQUAL HOUSING LENDER