COMPUTER BUSINESS CONSULTANTS, INC.

SECURITY

Best Practices

DO

- Use long complex passwords. 10-12 characters, with at least one capital letter, one special character, and one number.
- Use multiple authentication methods, such as text verification, when possible.
- Change passwords often and use different passwords for each login.
- Use a password management program to securely store and maintain strong unique passwords.
- Only connect to a password protected, secure Wi-Fi.
- Enable firewall protection.
- Always use encryption when storing or transmitting sensitive data.
- Limit third-party access to your devices.
- Be suspicious of any official-looking email message or phone calls that asks for personal, login, or financial information. When in doubt, contact the organization yourself using its legitimate contact information found online or on account documents.
- Always verify the "From" address in an email to ensure the domain matches the source it claims to be from.
- Hover your mouse over links in emails to check the actual destination URL.
- Lock your devices with a PIN or password when unattended and set devices to auto-lock when idle.

DON'T

- Share your password or login ID with anyone.
- Use the same password for everything.
- Download from untrusted sources.
- Email sensitive data, store sensitive files or information in your Email box. Permanently delete them. Email is not secure.
- Allow unknown partners and vendors to make a remote connection to your devices.
- Give out personal or financial data such as your Social Security number, account numbers, or login credentials in response to an email or an unsolicited phone call. An organization contacting you on legitimate business will not ask you for such information.
- Click links or call phone numbers provided in an unsolicited email or a suspicious website pop-up.
- Immediately trust an email because it features a company's real branding or appears to come from someone you know. It could be spoofing or a hack of a trusted email account.
- Trust a caller because they say they are your IT support, company vendors, or even an unknown coworker requiring access or asking for login information. Hackers often use social engineering of your trust to gain access.
- "unsubscribe" – it's better to mark the email as "SPAM" or "Junk" than deal with the security risks associated with clicking on the "unsubscribe" link, or responding to an email.

www.ComputerBusiness.com

940 W. Oakland Avenue, Suite A8, Oakland, FL 34787 • Toll Free: 800-778-0838 • Atlanta: 770-587-1199 • Orlando: 407-654-5600