CYBERSECURITY FOR SMALL BUSINESSES

In today's world, it's important for business owners to be vigilant in protecting their computer systems and data. Here are tips to help business owners and their employees protect themselves and their companies from losses and other harm.

- **Protect computers and Wi-Fi networks.** Equip your computers with up-to-date anti-virus software and firewalls to block unwanted access. Arrange for security software to automatically update. If you have a Wi-Fi network for your business, make sure it is secure, including having the router protected by a password that is set by you (not the default password).
- **Patch software in a timely manner.** Software vendors regularly provide "patches" or updates to their products to correct security flaws and improve functionality. Download and install these software updates as soon as they are available.
- **Set cybersecurity procedures and training for employees.** Consider reducing risks through steps such as pre-employment background checks and clearly outlined policies for personal use of computers. Limit employee access to only the data systems they need for their job, and require permission to install any software. Train employees about cybersecurity issues, such as suspicious or unsolicited emails, asking them to click on a link, open an attachment or provide account information.
- **Require strong authentication.** Ensure employees and other users connecting to your network use strong user IDs and passwords for computers, mobile devices and online accounts by using combinations of upper and lowercase letters, numbers and symbols that are hard to guess and changed regularly.
- **Secure the business's tablets and smartphones.** Mobile devices can be a source of security challenges, especially if they hold confidential information or can access your company's network. Require employees to password-protect their devices, encrypt their data and install security apps to prevent criminals from accessing the device while it is connected to public networks. Develop and enforce reporting procedures for lost or stolen equipment.
- **Back up important business systems and data.** Do so at least once a week. For your backed up data, remember to use the same security measures (such as encryption) that you would apply to the original data. In case your main computer becomes infected, regularly back up sensitive business data to additional, disconnected storage devices.
- **Use best practices for handling card payments online.** Seek advice from your banker to select the most trusted and validated tools and anti-fraud services. This may include using just one computer or tablet for payment processing.
- **Be vigilant for early signs that something is wrong.** Continuously monitor your bank accounts and card transactions. Identifying suspicious activity as early as possible can significantly decrease your liability during fraudulent situations.

Heritage BANK

Information provided by the FDIC