Huntington Welcome.

Help Protect Sensitive Data: Yours and Your Customers'

For businesses, it's vital to protect your company's information and your customers' data. Having a sound security plan, well-trained employees, and up-to-date software and hardware will go a long way to keeping valuable data from falling into the wrong hands.

☐ **Help protect against viruses, spyware and other malicious code.**

- Make sure each company computer/device is equipped with anti-virus software and anti-spyware. Configure all software to install updates automatically.

☐ **Take steps to secure your networks.**

- Safeguard your Internet connection by using a firewall and encrypting information. If you have a Wi-Fi network, make sure it is secure and hidden. To hide your Wi-Fi network, set up your wireless access point or router so it does not broadcast the network name, known as the Service Set Identifier (SSID). Password-protect access to the router.

☐ **Establish security policies to help protect sensitive information.**

- Create and enforce policies on how employees handle personally identifiable information and other sensitive data. Clearly outline the consequences of violating your cybersecurity policies. Educate employees on the safe use of social networking sites. Employees should know how to post content online without revealing private data or trade secrets. Hold employees accountable to your security policies and procedures.

☐ **Require employees to use strong passwords and to change them often.**

- Implement multifactor authentication that requires additional information beyond a password to gain entry. Check with your vendors that handle sensitive data, especially financial institutions, to see if they offer multifactor authentication for your accounts.

☐ **Employ best practices on payment cards.**

- Work with your bank or card processor to ensure the most trusted and validated tools and anti-fraud services are being used. You may also have additional security obligations related to agreements with your bank or processor. Isolate payment systems from other, less secure programs and do not use the same computer to process payments and surf the Internet.

☐ **Backup important business data and information.**

- Regularly back up the data on all computers. Critical data includes word processing documents, electronic spreadsheets, databases, financial files, human resources files, and accounts receivable/payable files. Back up data automatically if possible, or at least weekly, and store the copies either offsite or in the cloud.

63%

of confirmed data breaches leverage a weak, default or stolen password [1]

400+

businesses are targeted by business email compromise (BEC) scams every day [2]

59%

of employees steal proprietary corporate data when they quit or are fired [3]

1 Source: Americans and Cybersecurity. Pew Research Center.

2 Source: TRUSTe/National Cyber Security Alliance U.S. Consumer Privacy Index 2016.

3 Source: Q4 2016 & Year Review. Threat Summary. Proofpoint.

☐ **Control physical access to computers and network components.**

- Prevent access or use of company computers/devices by unauthorized individuals. Laptops are particularly easy targets for theft or can be lost, so lock them up when unattended. Make sure a separate user account is created for each employee and require strong passwords. Administrative privileges should only be given to trusted IT staff and key personnel.

☐ **Create a mobile device action plan.**

- Mobile devices can create significant security and management challenges, especially if they hold confidential information or can access the corporate network. Require users to password-protect their devices, encrypt their data, and install security apps to prevent criminals from stealing information while the device is on public networks. Be sure to set reporting procedures for lost or stolen equipment.

☐ **Protect all pages on your public-facing websites.**

- It's not just sign-up and check-out pages that need to be protected from attack. Work with your IT team to review policies allowing users to upload files, using HTTPS security protocol and SSL encryption, removing auto-fill from online forms, and hiding admin pages from search engines.

Contact Huntington

If you receive a suspicious email, call or text, or think your account data has been compromised, let us know. We'll help you determine the legitimacy of suspicious messages and account activity.

PHONE: **(800) 480-2265**

EMAIL: **ReportFraud@huntington.com**

For more information about phishing or your privacy and security, go to huntington.com/Privacy-Security.

Spotlight on Phishing

Educate employees about cyber threats.

- Phishing schemes aren't limited to individuals. Educate your employees on the telltale signs of phishing, such as unfamiliar senders, strange domain names, spoofed web pages or emails, and messages with links or attachments that you didn't request. Even employees inside your company, known vendors and C-suite executives can have their emails spoofed.
- Common spoofs include fake invoices, shipping information and W-2 forms as well as requests to send money.
- To reduce the risk of employees clicking on malicious links in external emails, make changes to the way links appear in emails from external sources, such as disabling them until the employee has the opportunity to further investigate a link.
- Flagging external emails with special text in the subject line or upper body of the email can help make someone look twice before opening the email or downloading an attachment.

For more information, go to **huntington.com/Privacy-Security**.