Tennessee State Bank
"Banking at its Best"
Member FDIC

Commercial Services Security Newsletter

December 2023 | CSN – Q4 - 2023

FS-ISAC

Preventing Fraud During the Holiday Season

"Cybersecurity has become a top concern for small and medium enterprises (SMEs) and nearly half (48%) of SMEs have experienced at least one cyber incident in the past year." (InfoSecurity Magazine) and "thousands of small and medium businesses (SMBs) have been harmed by ransomware attacks, with small businesses three times more likely to be targeted by cyber criminals than larger companies, and the total cost of cybercrimes to small businesses reached $2.4 billion in 2021." (Forbes)

Loss Prevention Tips

Implementing anti-fraud and cybersecurity processes will help you incorporate controls and prevent fraud.

1. Verify invoices. Employ procedures to verify any incoming invoices before payment. Compile a listing of all suppliers with whom you normally do business by name, address, and phone number, and make the list available to anyone responsible for the payment of your invoices.

2. Educate your employees. Make your workers aware of the most common types of scams against small businesses. Obtain pamphlets and literature concerning small business fraud from your local police agency or consumer affairs bureau. Post this information at your business.

3. Don't buy over the phone. Unless you have a previously established relationship with a supplier of business or office supplies, never make orders or purchases over the phone. Scammers sometimes obtain the names of business employees and assert that these persons have placed orders on behalf of the business. Instruct your employees to verify the order with the person who placed it.

4. Ask for verification of offers in writing. If a caller makes an offer regarding the provision of goods or services that interests you, request that the offer be made in writing and forwarded to you for review. Be wary if the caller refuses to forward this information to you or to otherwise provide references.

5. Beware of prizes or "free trial" offers. Small business scam artists often offer prizes or "free" gifts as an inducement for the business to purchase their products. Be aware that these "prizes" are usually overpriced or are of inferior quality. In addition, by agreeing to a "free trial" offer you may be unwittingly enrolling in a negative option plan, in which you will be charged monthly until the enrollment is canceled.

6. Beware of solicitations that appear to be bills or official mailings from federal, state, city, or county governments. Before sending payment or providing personal or confidential information, confirm with the government entity that the mailing is legitimate, and any document being purchased is required to conduct business. Pay special attention to the fine print and look for disclaimers that may indicate that the mailing is a solicitation or that the document offered is unnecessary. Also, be wary of any company whose staff uses high-pressure sales tactics to convince you that your business needs a particular document to continue doing business.

7. Do not be influenced by a money-back guarantee. While a money-back guarantee is nice to have, these guarantees are only as good as the companies offering them.

Did You Know?

- Fingerprint research shows that triangulation fraud already has a significant financial impact on the e-commerce industry, and its effects will continue to grow. Experts estimate that card-not-present (CNP) fraud losses, including triangulation fraud, will exceed $10 billion in the US alone by 2024, making up 74% of all fraud.
- Chargeback fees cost between $20 and $100, depending on the merchant's agreement with their acquirer. When you add these fees up with all the other hidden and indirect costs, companies often lose more than twice the transaction amount for each chargeback (Chargeback Gurus).

Cybersecurity Tips

1. Train employees in security principles. Establish basic password and security policies for employees, such as requiring strong passwords, and establish appropriate internet use guidelines that detail penalties for violating company cybersecurity policies. Establish rules of behavior describing how to handle and protect customer information and other vital data. A clean desk policy can also be part of protecting data.

2. Protect information, computers, and networks from cyber attacks. Keep clean machines: having the latest security software, web browser, and operating system is the best defense against viruses, malware, and other online threats. Set antivirus software to run a scan after each update. Install other key software updates as soon as they are available.

3. Provide firewall security for your internet connection. A firewall is a set of related programs that prevent outsiders from accessing data on a private network. Make sure the operating system's firewall is enabled or install free firewall software available online. If employees work from home, ensure that their home system(s) are protected by a firewall.

4. 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 phone is on public networks. Be sure to set reporting procedures for lost or stolen equipment.

5. Make backup copies of important business data and information. Regularly backup the data on all computers. Critical data includes word processing documents, electronic spreadsheets, databases, financial files, human resources files, and accounts receivable/payable files. Backup data automatically if possible, or at least weekly, and store the copies either offsite or in the cloud.

6. Control physical access to your computers and create user accounts for each employee. Prevent access or use of business computers by unauthorized individuals. Laptops can be 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 requires strong passwords. Administrative privileges should only be given to trusted IT staff and key personnel.

7. Secure your Wi-Fi networks. If you have a Wi-Fi network for your workplace, make sure it is secure, encrypted, 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). Passwords protect access to the router.

8. Employ best practices on payment cards. Work with banks or processors to ensure the most trusted and validated tools and anti-fraud services are being used. You may also have additional security obligations under 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.

9. Limit employees' access to data and information, and limit authority to install software. Do not provide any one employee with access to all data systems. Employees should only be given access to the specific data systems that they need for their jobs and should not be able to install any software without permission.

10. Passwords and authentication. Require employees to use unique passwords and change passwords every three months. Consider implementing multi-factor 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 multi-factor authentication for your account.

If You Think You've Been Scammed

If you suspect your business has fallen victim to a scam:

- Contact us immediately so we can act and provide recommendations
- Report suspicious activity to the Internet Crime Center, www.ic3.com, and/or your local law enforcement agency.

© 2023 FS-ISAC, Inc. | All rights reserved