SECURITY WATCH NEWSLETTER

Vol. 7, Number 1

Safe Internet Browsing: Secure Your Browser

Cybercrime is a growing threat to corporations and consumers who are increasingly using online methods to run their businesses and lives. Exploiting vulnerabilities in web browsers is a popular way for attackers to compromise computer systems. Web browsers are designed to store information for your convenience, but that information can also fall into the wrong hands.

All kinds of personal information, from your IP address, location, work hours, habits, banks, applications, and even passwords are there for the taking. If you store your login credentials in webforms or the browser's password manager, your credentials would be available to anyone looking for them. An attacker can easily compile this information into a web dossier that can lead to identity theft, financial losses and ransomware.

The key to online safety is browsing with care.

Customize your browser security settings and preferences to help protect yourself while using the Internet. When using browsers in their default mode, one wrong click in a search engine or one malicious advertisement loading on your favorite website is all that it takes to fully compromise your system. Here are some ways you can use your browser to protect yourself.

- **Disable autofill** to ensure your form history is not saved locally for potential exploitation.
- **Disable the option to save your login information** to make it unavailable to attackers.
- **Regularly clear your browsing history** as it lessens the amount of data available to attackers.
- **Use a third-party password manager** to make it easier for you to manage complex passwords and more difficult for attackers to access.

Additionally, think before you respond to unexpected pop-up windows. Never provide sensitive information unless you initiated the communication and you are sure you know with whom you're interacting. Make sure you're at the correct website and that the site you landed on isn't a fake. It's better to type the URL into your browser because clicking on a link provided on a web page or in an email could send you to a site that has been seeded with malware. When logging into a website or when providing sensitive information, ensure the web page is secure by looking for a web address with https ("s" stands for secure) and a closed padlock beside it. (The lock might also be in the lower right portion of the window.)

These are just a few ways to defend yourself online. Because we share a lot of personal information online, including credit card numbers and social security numbers, it's prudent to learn how to protect yourself from scams and hackers.

Trustmark National Bank
Offices in Alabama, Florida, Mississippi, Tennessee & Texas

Types of Fraud Targeting Small Business

Scam artists and cyber criminals do not discriminate. Any company that uses a computer to conduct their business is at risk of a cyber attack. It's important that you and your employees know how to identify a scam before your business falls prey.

Here are some common scams:

- **Spear phishing:** Spear phishing is a type of phishing attack where a cybercriminal targets an individual or group. Spear phishing attacks are among the hardest to differentiate from actual email correspondence because the attacker includes information that is familiar to the victim.
- **Account takeover:** This is a type of business identity theft where cyber thieves gain control of a business' bank account by stealing employee passwords and other valid credentials. Thieves can then initiate fraudulent wire and ACH transactions to accounts controlled by the thieves.
- **Fake invoicing:** Scam artists try to trick businesses into paying for products or services that they didn't order, that have little or no value, or that are never delivered. Also, if a scammer gains access to a business email account, they can intercept and edit incoming emails from companies you work with, like suppliers, and issue fake invoices.
- **Fraudulent transactions:** By using a stolen payment card in a transaction, scammers try to obtain goods without paying for them. Merchants can be left holding the bag when the credit card provider issues a chargeback on the account that was used fraudulently.
- **Compliance services:** Scammers send solicitations that appear to be official mailings from a government agency and imply the business is required to pay a fee to comply with annual meeting, minutes or reporting requirements. Often, the business can comply with official requirements on its own for free or for a fraction of the cost.
- **Unsolicited services or products:** Scammers often send products or provide services followed by an invoice for an excessive amount of money. A common example is fake phone book company asking to update your listing. After receiving the info, they'll send an invoice.
- **Fake SEO (Search Engine Optimization) experts:** Posing as an SEO expert, a scammer presents to a small business a plan for increasing its ranking on Google. The scammer will take the business' money and not do the work.

Fraud is an ongoing, ever evolving threat that can be detrimental in the small business world. It's important that businesses protect their hard work by raising fraud awareness among employees and taking tangible precautionary measures.

HIGHEST CUSTOMER SATISFACTION
J.D. POWER AND ASSOCIATES
RETAIL BANKING · SOUTH CENTRAL · 2018
PRESENTED TO
TRUSTMARK NATIONAL BANK
BY J.D. POWER AND ASSOCIATES