



## Securing your data: advice from an award-winning cybersecurity team

*Written by: Fred Hamilton, Chief Information Security Officer, BHG Financial*

Technology continues to insinuate itself into almost every facet of our daily lives, whether it is personal or work-related. As a result, protecting data privacy has become increasingly more relevant to every consumer and business. In 2022, 422 million people were affected by data breaches at U.S. companies at an average of 4.8 breaches per day.<sup>1</sup> Stolen data included bank account numbers, medical histories, Social Security numbers, and more. Personal data is continuously being collected, shared, or sold, so it is crucial that everyone understands how to protect it.

In today's world, it is incumbent upon companies to ensure they have the information security protocols in place to protect customer data and electronic assets from the growing global threat of hackers. This requires a keen focus on increasing the adoption of new technological innovations and following industry-best practices in the evolving world of cybersecurity.

Companies with an established history of successfully safeguarding electronic data often share similar characteristics, such as:

- A significant investment in people and technological resources
- Executive leadership that has demonstrated its mission to make information security and data privacy top priorities
- Next-generation firewall and encryption technology to protect internet connections and Wi-Fi networks
- Best-in-class security software installed and updated automatically
- Industry certifications and acknowledgments that appropriate security controls are in place to protect the confidentiality, integrity, and availability of all data assets

BHG Financial is a noteworthy financial services provider that has earned recognition for its exceptional cybersecurity capabilities. The company boasts a team of seasoned cybersecurity professionals who have been recognized for their outstanding contributions to the industry. In this article, we will be sharing insights from BHG Financial's cybersecurity experts on simple yet critical tasks that businesses should not overlook.

In acknowledgment of its dedication to cybersecurity, BHG and its Information Security Team recently received several industry accolades. First, it was honored with a 2022 Fortress Cyber Security Award for organizational excellence.<sup>2</sup> In addition, the company has been certified SOC 2<sup>®</sup> Type 2 compliant in accordance with standards set forth by the American Institute of Certified Public Accountants. SOC for

---

<sup>1</sup> Source: <https://explodingtopics.com/blog/data-privacy-stats>

<sup>2</sup> Source: <https://www.bintelligence.com/blog/2022/6/7/100-named-in-2022-fortress-cyber-security-awards>

service organizations is a compliance standard which demonstrates that BHG Financial is safeguarding customer data throughout its services and is meeting standards for strong operational effectiveness.

### **Security tips to protect your data from BHG Financials' Security Team**

- In the spirit of driving awareness about the importance of being cyber-aware, and to help you protect the integrity of your data, here are some simple tips not to be overlooked: Avoid uploading sensitive or confidential data (personal or customer account information, Social Security numbers, etc.). If you must, all information should only be uploaded to a trusted, secure source or database.
- Be aware of any suspicious emails and do not click on unfamiliar embedded links. Be especially wary if an email contains misspelled words within the body and/or subject line of the message. Other suspicious indicators include unfamiliar email domains or enticements to act or respond immediately. Report these emails to your organization's IT Support team right away.
- Lock your screen when you are away from your desk to prevent others from accessing sensitive information.
- Beware of public Wi-Fi. It can expose your data to scammers monitoring internet activity. It also greatly increases the risk of malware being transferred to your devices. If you must access a public Wi-Fi network, use a virtual private network (VPN) to add a helpful layer of security.
- Find out if your personal information has been targeted in a data breach. It is quick and quite easy to do. Simply enter your email or phone number at <https://haveibeenpwned.com/>. The system will respond almost immediately, detailing when and where your data was breached.
- Before disposing of old IT equipment, ensure no personal data remains on the system. Consider hiring a specialist to wipe the data from the device or use deletion software such as BitRaser File Eraser or File Shredder.

### **Your role in data privacy**

Cybersecurity is everyone's business. With a little discipline and practice, protecting the integrity of your data can become second nature. Nobody wants to be the person who accidentally downloads malware onto their company's systems, or who leaves their online banking credentials vulnerable to external threats. Following and regularly repeating a few simple security protocols is well worth the time to remain cyber safe at home and at the office.