March 2024

Small Business Bulletin

Provided by B_Officialname

Cybersecurity Best Practices

Cyberattacks are becoming more frequent and complex, and businesses of all sizes and industries are potential targets. In fact, cybercriminals increasingly go after small businesses since they contain much of the same types of sensitive information as larger enterprises but often have weaker cybersecurity defenses. Verizon's 2023 Data Breach Investigations Report found that 43% of all cyberattacks target small businesses, and 60% of those victims go out of business within six months of the attack.

Even if a small business survives a cyberattack, there can still be devastating consequences, such as high costs, reputational damage and unanticipated downtime. To best combat these risks, it is important for small business owners to be aware of common cyberthreats they may face, including:

- **Phishing**—Phishing is a type of cyberattack that utilizes deceptive emails or other electronic communication to manipulate recipients into sharing sensitive information, clicking on malicious links or opening harmful attachments. Emails are the most common delivery method for phishing attempts, but cybercriminals may also use text messages, social media messages, fake or misleading websites, voicemails or even live phone calls.
- **Business email compromise (BEC)**—A BEC scam entails a cybercriminal impersonating a seemingly legitimate source—such as a senior-level employee, supplier, vendor, business partner or other organization—via email. The cybercriminal uses these emails to gain the trust of their target and trick them into wiring money, sharing sensitive information or engaging in other compromising activities.
- **Malware**—Malware is a general term that describes viruses, worms, Trojan horses, spyware, adware, rootkits and other unwanted software or programs. Once a malware program has gained access to a device, it can disrupt normal computing operations, collect information and control system resources.
- **Insider threats**—Workers who have access to sensitive information, including contractors with access to the company's network, may be aware of existing security weaknesses and can exploit them more easily than outsiders.
- **Password attacks**—Using weak or easily guessed passwords or using the same password for multiple accounts can result in compromised data.

To limit the risk of cyberattacks, small business owners should implement the following cybersecurity best practices:

- **Employee education**—Workforce cybersecurity education is essential to teach employees to identify phishing attacks, social engineering and other cyberthreats.
- **Security software**—A network firewall can prevent unauthorized users from accessing company websites, email servers and other sources of information accessed through the internet.
- **Multifactor authentication (MFA)**—Important accounts, including email, social media and banking apps, should require MFA to limit the opportunity for cybercriminals to steal data.
- **Data backups**—Essential files should be backed up in a separate location, such as on an external hard drive or in the cloud.

As cyberthreats become more frequent and severe, small businesses should take protective measures to secure all company, personal and financial information.

fifs Franconia Insurance & Financial Services

KEYSTONE

© 2024 Zywave, Inc. All rights reserved.

Common Employee Communication Mistakes to Avoid

Effective communication is crucial to fostering a positive relationship between employers and employees. It can show employees they're valued and heard, improving employee satisfaction and retention. Conversely, poor communication can lead to workplace inefficiencies, foster employee discontent, and create engagement and retention issues. These concerns can significantly impact workplace productivity and organizational revenue; according to a 2022 study by Grammarly and the Harris Poll, organizations lose about $1.2 trillion yearly due to ineffective communication. For small businesses, even a marginal decrease in productivity or revenue can be devastating.

To combat the consequences of poor communication, this article provides an overview of common employee communication mistakes and discusses how small businesses can avoid them.

Benefits of Effective Communication

The purpose of employee communication is to keep employees informed. This is important at all levels, including groundbreaking business information as well as day-to-day interactions. Organizations that effectively communicate with employees may experience the following benefits:

- Increased productivity
- Improved retention
- Greater employee engagement
- Improved workplace safety and crisis management
- Better success rates for change initiatives
- Increased efficiency
- Improved collaboration
- Increased knowledge-sharing and innovation

Common Employee Communication Mistakes

Despite the significant role employee communication plays in creating successful and efficient workplaces, research indicates that many employers still struggle to convey important information to workers effectively. A 2022 report by Gallup found that just 7% of U.S. workers strongly agree that communication at their organizations is accurate, timely and open. This can significantly impact company culture, employee morale and performance. Employers can make several common mistakes when it comes to employee communication, including:

- Providing infrequent and inconsistent communication
- Failing to understand the employee audience
- Providing irrelevant and impersonal information
- Lacking a clear internal communication strategy
- Not asking for employee feedback
- Using the wrong communication channels
- Overloading employees with information
- Not measuring the effectiveness of internal communications

Improving Employee Communication

There are many ways for employers to connect with employees to enhance engagement, productivity and profitability. The most effective communication strategy is tailored to align with an organization's and its employees' unique goals and needs. Small businesses can consider the following guidance for effective communication with employees:

- Identify the goal of the communication.
- Understand the audience.
- Tailor messaging to the audience and objective.
- Create avenues for employee feedback or questions.
- Measure performance of the communication strategies.

Conclusion

Employee communication can significantly impact employer-employee relationships. Small businesses should consider how these tips can apply to the structure of their organizations. Employers who enable better communication among employees may notice improvements to their bottom lines.

Contact us today for more information.