2024

Issue 7 Volume 14

frogworks

Managing Your Technology So Your Business Doesn't Croak.

Ribb"IT" Review

INSIDE THIS ISSUE:

The Importance of IT Support for Small Businesses

Businesses rely on technology to operate smoothly. Computers, networks, and various software applications are essential for daily tasks. However, technical problems can arise at any time, disrupting business operations. This is where IT support plays a crucial role. IT support helps ensure business continuity and addresses technical issues effectively.

What is IT Support?

IT (Information Technology) support involves various services that assist users in resolving technical problems. IT support teams work behind the scenes to keep technology running smoothly. They handle everything from fixing computer glitches to maintaining servers and networks.

How IT Support Ensures Business Continuity

Preventing Downtime

IT support teams monitor systems to detect and resolve issues before they cause major disruptions. They perform regular maintenance, update software, and apply security patches. This proactive approach helps prevent problems that could lead to downtime.

This monthly publication provided courtesy of:
Alex Bleam,
Owner of Frogworks

How IT Support Ensures Business Continuity

Data Backup and Recovery

One of the most critical aspects of business continuity is data backup. IT support ensures that all important data is backed up and can be restored if needed.

Disaster Recovery Plans

IT support helps develop and implement disaster recovery plans. A well-thought-out disaster recovery plan includes procedures for data recovery, alternative communication methods, and ways to continue operations during a crisis.

Cybersecurity

IT support teams prioritize protecting businesses from cyber threats. To safeguard sensitive information, they implement security measures such as firewalls, antivirus software, and encryption. Regular security assessments and employee training also help reduce the risk of cyberattacks.

Help Desk Support

Many businesses have a help desk where employees can report technical problems. IT support staff at the help desk troubleshoot and resolve software errors, network connectivity problems, and printer malfunctions. Quickly resolving these problems helps employees stay productive.

Remote Support

With advancements in technology, many IT support tasks can be performed remotely. Remote support allows IT technicians to access and fix computers from a different location.

Hardware and Software Management

IT support is responsible for managing hardware and software assets. This includes installing new software, upgrading hardware, and ensuring all systems are compatible. Proper management of these assets prevents technical issues that could disrupt business operations.

User Training

Technical problems often arise from user errors. IT support trains employees to use software applications and follow best practices. Educated users are less likely to encounter technical issues, and when they do, they are better equipped to handle them.

In conclusion, IT support is vital for maintaining business continuity and addressing technical issues. By preventing downtime, ensuring data backup and recovery, developing disaster recovery plans, and protecting against cyber threats, IT support helps businesses stay operational during disruptions. Additionally, help desk support, remote assistance, hardware and software management, and user training ensure that technical issues are resolved quickly and efficiently.

The Importance of Security Awareness for Employees

Just think of all the sensitive information your business competitors or hackers would love to handle. From simple identity theft to ransomware attacks on your business systems, a little security awareness goes a long way. In fact, it could save your business a world of trouble, say, when an educated employee's finger freezes over the mouse instead of clicking through to a bad link.

Is Your Business Cybersecurity Aware?

Big and small businesses alike need online defenses, from firewalls and encrypted software to strong passwords and password managers. Still, can you imagine putting in all that work just to have one employee slip up and unknowingly hand over the wrong information to the wrong individuals?

Security breaches exploit your company or customers' credit card information, addresses, names, and more to sully your reputation or profit in other ways. Unfortunately, because humans are infallible and hackers are always evolving their efforts, breaches happen more often than a business owner might realize. Thankfully, you can step up your defense strategy with cybersecurity awareness training.

Empower Your Employees With Cybersecurity Awareness Training

According to Verizon, about 68% of breaches in 2023 involved a non-malicious human element (individuals fell victim to attacks or made errors). In cases where the hacker demanded ransomware, each breach left the affected companies with a $46,000 average loss. Interestingly, eight out of these nine companies did not have a cybersecurity awareness program in place.

What might your business include in security awareness training topics? Ideas include:

- Educational scripted videos.
- Generic presentations covering typical programs your company uses.
- Cyber tests that update your employees on all modern-day attacks and threat types.

Your business might also want to update the training topics as cybersecurity practitioners note threat trends.

The Importance of Security Awareness for Employees

How Digital Security Training Assists Your Company

There's a lot to be said for adding a layer of security that simultaneously empowers your employees to recognize and thwart cyberthreats. Here are a few notable benefits your business might enjoy with a security awareness training program in place:

Prevent Data Breaches from Malicious Activity

Has a hacker sent out a faux email or imitation website login page? Your security-aware employees won't open them or fill in sensitive data. Trained employees will also know to look for certain features like phishing attempts with misspellings or suspicious links.

Put Up Cyber Defenses

Awareness helps with observing malicious activity and understanding protocols, but training also creates a much stronger defensive line with stronger passwords and multi-step authentication. You could even outline GDPR and HIPAA compliance so that employees bar threats before they even begin.

Boost Business by Putting Your Customers at Ease

Vercara's 2023 research showed that about 66% of customers would not do further business with a company after a data breach. About 44% of those survey participants believed that a company only falls victim to these attacks without adequate cybersecurity in place.

If your customers fear their credit card information, email and home addresses, and other personal information are vulnerable with you, they'll leave. With security awareness training, your business may find that developing a culture of safety and security also streamlines this human risk management factor.

We Have an E-Newsletter!!!

Do we have your e-mail address??? If you would like to receive our newsletter though email please visit us at:

www.getfrogworks.com/newsletter