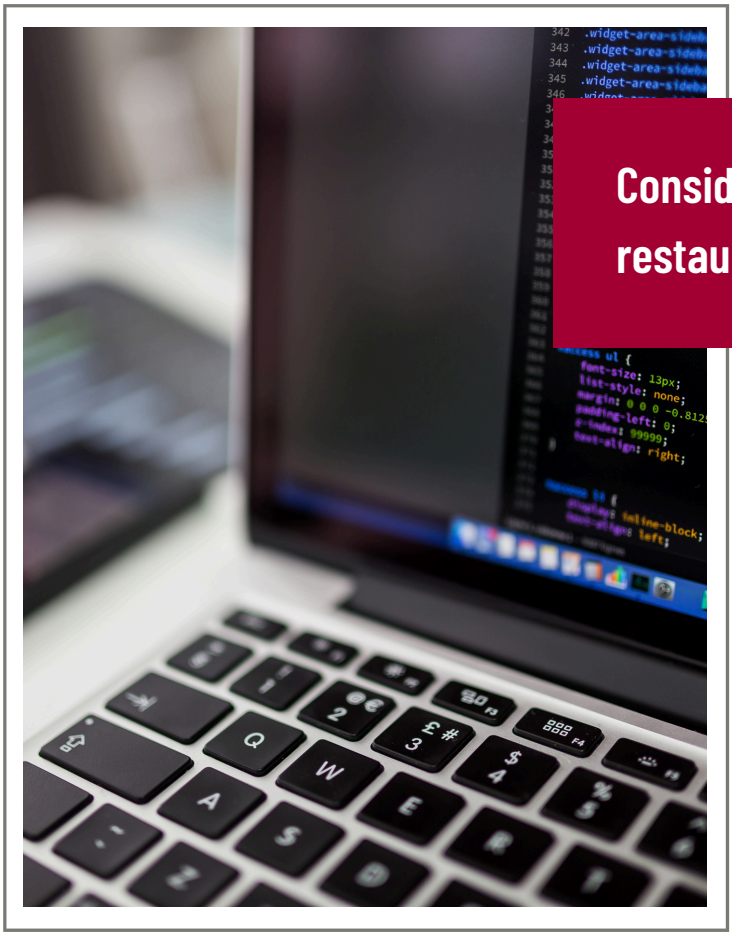
IT Best Practices for Restaurant Franchises



By: Cheyne Statezny, IT Support Specialist

Consider these tips to protect your restaurant franshise infrastructure

Workstation Security

Cybersecurity

Phishing Awareness

Data Backups

KerberRose

YOUR TRUSTED ADVISOR ®

More than 40 years of experience & featuring 13 convenient locations throughout Wisconsin and the Upper Peninsula. Visit our website to learn more:

www.kerberrose.com

Operating a restaurant franchise can present many unique challenges; however, IT best practices apply to every business. Any data integral to the business (i.e. employee records, payroll information, accounting information, etc.) are among any business' most valuable confidential information.

There are a few IT best practices which are easily implemented and vastly strengthen a business' IT infrastructure and can protect franchisees from unnecessary risk.

Workstation Security

Every workstation with access to business data — whether an on-site desktop, a laptop, or a mobile device like a tablet or smartphone — needs to be as secure as possible.

For a desktop, all users who have access to the device should be using a separate account to log in (this extends further to specific account logins, like email or payroll services too). Providing each user with a separate login offers an extra element of security. Each user's access can be limited to only the applications and information they absolutely need, while preventing them from accessing data they shouldn't see. This also provides a built-in audit mechanism as any changes to shared documents are tied to one person's account — any tasks completed are tied to the specific user.

Conversely, shared accounts could allow users to retrieve or edit sensitive data they shouldn't see, or make unauthorized changes to applications and documents.

Likewise, mobile devices should be password/passcode protected. Of course, this is recommended for everyone — especially business owners and management who may access data from their smartphone. Should a device fall in the wrong hands, a password will prevent unauthorized access to the data.

All passwords for desktops mobile devices, and individual applications should be long, complex unique, and memorable. Attackers can use a variety of software tools to guess a password, so the simpler the password, the more quickly it can be hacked. A strong password does not include the user's name or any personal identifier.

Password Security Checker

Strength	Example
extremely poor	password
poor	1234password
moderate	12beatles!
strong	B3atl3s!#65
extremely strong	Y3ll0w5ubMarin3#!?

Cybersecurity

Antivirus software has the primary goal of detecting and removing (or otherwise disabling) viruses and other forms of malware. Computers can become infected with malware in a variety of ways — downloaded inadvertently by a user, embedded within other software or files, or implanted by unsecure websites, to name a few. Viruses can accomplish different goals for attackers, such as: exposing sensitive data, holding data for ransom, or generally wreaking havoc on the infected computer.

Antivirus (AV) apps typically are "ever-present" — they run automatically and persistently whenever the computer is powered on. This allows AV software to constantly monitor the computer's file system which it scans for malicious files (some AV software also automatically scans new downloaded files, as well as web pages, emails, and more). When a malicious file is detected, the AV software will (either automatically, or with user input) remove or destroy the malware.

AV software relies on never-ending efforts by cybersecurity experts to ensure virus definitions keep up with advancements by attackers. Stated another way, cybersecurity experts are constantly racing to keep up with new attack methods. Thus, antivirus software must be updated frequently and regularly to ensure maximal efficacy.

Many different anti-virus and anti-malware solutions are available, each with varying costs and benefits. Industry leaders include AVG, Kaspersky, McAfee, Norton, and Trend Micro. Windows 10 also includes Windows Defender, which is Microsoft's built-in anti-virus and security software. Additional solutions (including some which are free) are also available, although may be less effective. Each possible AV solution should be thoroughly researched before making a selection.

Phishing Awareness

Phishing is an attempt by an attacker to send a legitimate-appearing email seeking some type of information. Some phishing attacks include links which appear to point to trusted sites, but may download viruses or malware, or may ask for a sign-in, which would give the attacker the target's sign-in credentials — giving an attacker access to sensitive information. Some phishing emails may come with attachments, which are actually malware disguised as documents. Attackers may also masquerade as a co-worker, client, or trusted individual to glean information from you.

It is extremely important to be skeptical of any unexpected email. If any email appears to come from a trusted source seems suspicious, it should be investigated rigorously before its requests are granted. Likewise, an untrustworthy-appearing email from an unknown source should be thoroughly investigated. Ardent skepticism by all users is one of the strongest anti-phishing tools.

Data Backups

Businesses quickly accumulate important data — HR, payroll, and accounting data are mandated by law to be held for varying intervals. Every 1 gigabyte (GB) of data represents roughly 10,000 documents. As for a point of reference, most new smartphones have 128GB of space or more and larger businesses measure their data footprint in terabytes, each of which is 1,000GB.

That data, especially when represented as documents, is incredibly valuable and difficult to concretely evaluate. Even estimating conservatively, 1GB — 10,000 documents — represents 2,500 hours of labor to create

the documents. When factoring in the less tangible value of each document, such as the information it represents, the relationships each document maintains, and the potential losses that with coincide with losing the data, the cost of even a small amount of data is staggering.

Fortunately, the cost of data storage is incredibly low and every business should back up its data. Presented here are two options for backing up data: physical backups and cloud backups.

In a physical backup, data is copied to an additional physical storage device. The storage device itself can take a variety of forms: thumb drives, DVDs, SD cards, and external hard drives can all serve as physical backups. Obviously, portability is dependent on the size of the device; however, durability can vary as well. Physical devices have varying limits to the amount of data they can hold.

Some file storage devices are designed specifically with data backups in mind and come packaged with software which will automatically write copies of files onto it. Most devices will require the user to manually copy files or folders to ensure they are backed up.

Physical backups are not inherently secure, although measures can be taken to protect the data from falling into the wrong hands, like password protecting files and folders. Here, the portability of a physical backup can actually make it less secure, as some file storage devices are small and, thus, easily misplaced.

Data can also be backed up to the cloud — a network of file servers accessed via an internet connection. There are a few distinct benefits to choosing a cloud-based backup solution. First, cloud backups are at least as secure as the most secure physical devices. Data is encrypted and password protected, ensuring only users who are intended to access it can gain access.

Since cloud backups are not tied to a physical location, data can be backed up and retrieved anywhere the user has an internet connection. Data is backed up to the cloud automatically (or at the very least, at regular, short intervals), without user input, so backed up data is current and reflects any recent changes.

There is no practical limit to the amount of data a cloud backup solution can store; however, many backup solutions charge higher rates for more data. Still, the cost of cloud backup solutions is reasonable. Leading cloud storage solutions include CrashPlan and Microsoft's OneDrive.

While both a physical backup solution and a cloud backup solution can each be sufficient in backing up valuable (or indeed priceless) data, the benefits of a cloud backup solution make it the stronger option. To be clear, it is absolutely recommended to have some backup solution in place, even if it is a physical device.

Final Thoughts

Whether you are operating a large or small restaurant franchise, you should not have to worry about your data being at risk. By following these steps you and your franchise will be better equipped to defend sensitive information.

Our Trusted Technology Advisors will make sure you are well-equipped to both prevent and react to security breaches and lost data. You can visit our website at www.kerberrosetechnology.com to view our cybersecurity and data backup services, or contact KerberRose Technology for a free consultation to discuss what we can do improve your restaurant franchise infrastructure.