IT Best Practices for Retail Shops

Why IT matters in modern retail

- Retailers today rely on technological solutions to perform their day-to-day activities.
- From very small stores to supermarkets, retailers use technology to help process payments, control inventory and track sales.
- Typically, most retailers have a Point of Sale (POS) System at the front of their store that processes customers' purchases.
- In addition to being able to pay via a card through the use of a credit card terminal, many retailers use inventory management software and utilize WiFi from their register terminals to connect their staff's personal devices.
- Along with using POS Systems to process customer purchases, hundreds of retailers also have an online store linked to the same inventory control systems they have in their brick-and-mortar stores.
- When all these technologies run as designed, they help retailers serve their customers quickly and efficiently.
- If technology fails for any reason or becomes insecure, the retailer's ability to make sales would stop and/or the retailer's customers' personal data may be at risk.
- Retailers must have dependable and secure information technology (IT) infrastructure to maintain their operations and provide the highest level of customer service.

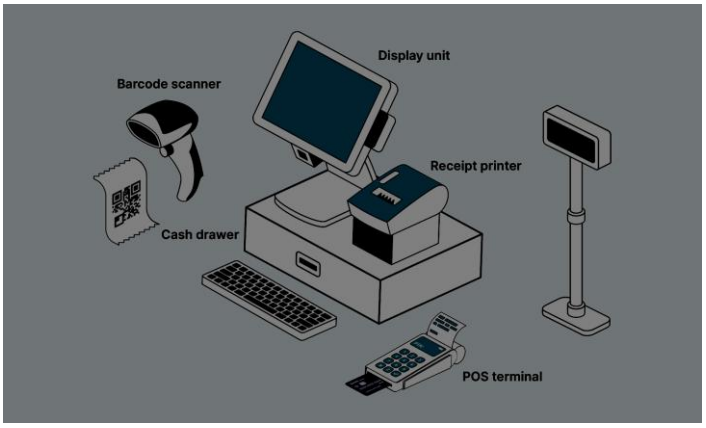
Typical technology used in retail shops

Point of Sale (POS) Systems

A point-of-sale (POS) system is the technology at checkout which records transactions, prints receipts and frequently connects directly to the store's inventory management system.

Modern POS systems frequently offer:

- Barcode Reader
- Reporting on sales
- Stock Management
- Tracking of customer purchases



Payment Terminals

Card payment terminals allow the consumer to pay by card, whether via debit, credit and/or contactless.

They must meet the security required by the Payment Card Industry Data Security Standards (PCI DSS).

Inventory Management Software

Retail inventory management systems keep track of goods currently held in stock along with listings of goods sold and how many units of each good were sold every time it is sold. Retail Inventory Management Software has prevented out-of-stock situations and aids in placing optimal orders.

E-Commerce Integrations

Many retailers now run an e-commerce website along with their brick-and-mortar store operation; e-commerce platforms commonly integrate directly with the POS system to maintain correct stock levels.

Customer Loyalty Systems

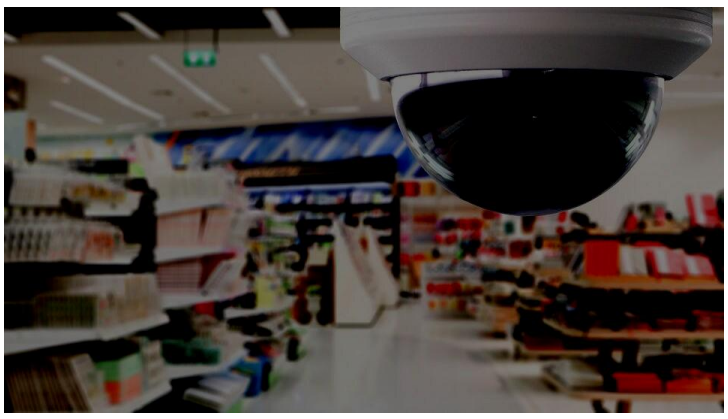
Loyalty Programs are used today by many retailers in order to capture customer buying habits and to provide discounts, rewards or benefits to consumers who use their loyalty program.

Sometimes loyalty programs also maintain customer's personal information such as name, email address, and buying history.

CCTV and Security Systems

Retail businesses protect themselves against theft by using security devices and surveillance cameras.

Digital CCTV systems save video footage to be accessed remotely.



Staff Tablets and Mobile Devices

Retail use hand-held mobile devices and tablet computers for better supply chain management, inventory lookup and to accept payments.

Shop Wi-Fi Networks

Retail stores often provide both wireless networks for store employees and for their customers.

Store wireless networks should be well-secured to minimise electronic security risks.

The most common IT problems in retail environments

Retail business are subjected to many of the same types of technology challenges.

The following outlines the most often experienced technology challenges:

1. **POS System Outages**

During peak business hours, point of sales system may fail to operate.

2. **Payment Processing Inaccuracies**

The card processing terminal system fails to connect to the processor during credit card transactions.

3. **Inventory System Inaccuracies.**

Due to poor inventory systems, physical inventory may not be recorded correctly.

4. **Slow or Unreliable Internet.**

Retail technology extensively relies upon the availability and reliability of the Internet.

5. **Security Vulnerabilities**

Vulnerable systems and insecure networks are at risk to expose sensitive information to unauthenticated or unauthorised individuals.

IT best practices for retail operations

Best practices for securing retail POS systems

- Update software automatically.
- Require unique, complex passwords and MFA.
- Have a dedicated network for POS.
- Quick win: Change the default password on the POS.

Create a separate Guest Wi-Fi network

- Have a Guest network for customers
- Have your POS and other stock on your Staff network.
- Quick win: Use the Guest feature of the router.

Regularly update software.

- Enable auto-updating of all POS, terminals, and devices.
- Check firmware at least once a month.
- Quick Win: Update overnight.

Device & Endpoint Security

- Use Microsoft Defender or equivalent product.
- Encrypt tablets or laptops.
- Quick win: Confirm the antivirus program is running.

Password Management/MFA

- Use Passphrases of at least fourteen characters in length.
- Use MFA on POS Admin and email.
- Quick win: Enable MFA on M365/Microsoft 365.

Secure Payment Processing.

- Use PCI compliant terminals.
- Do not store card details.
- Quick Win: Train staff to detect signs of fraud.

Role-based access for employees.

- Cashiers: Cash Drawer only.
- Managers: Inventory access.
- Quick Win: Review logins on a quarterly basis.

Monitoring System and Logs.

- Enable logging in your POS system.
- Verify unusual activities on a weekly basis.
- Quick Win: Set up email alerts for unusual activity in the POS.

Payment System Security

To securely process card transactions, merchants must staff and policies in accordance with PCI DSS standardisation and security practices. This means high-level processes must include the

- Use of a secure payment terminals provided by trusted merchant service providers;
- The encryption of processing transactions;
- Avoidance of raw storage of card data;
- Protection of POS devices by preventing tampering and/or mishandling

Merchants should also follow the advice and recommendations provided by their payment service providers.

Data Protection and Customer Information

Merchants collect personal information through loyalty programs, online purchases, and directly through customer service. Under GDPR in the UK, merchants must ensure;

- Only collect the personal data they absolutely need.
- Protect collected data using adequate security measures.
- Limit access to supported data to only authorised employees.
- Delete personal data when it is no longer required.

Merchants should make customers aware of how their personal data will be used.

Backup and Disaster Recovery for Retail Systems

Backing up data allows retailers to recover after a system failure or cyber incident.

Some of the most important systems to back up include:

- POS sales data
- Inventory records
- Financial systems
- Customer databases

Backup systems should be automated, secure and tested regularly.

Retailers should also consider how they will continue to trade temporarily in the event that their IT systems become unavailable.

Staff Access and Device Management

Access to systems should correspond to staff responsibilities.

Some best practices include:

- Role-based access control
- Deleting staff accounts when they leave the company

- Securing devices through the use of passwords or biometric identification

Practical IT Checklist for Retail Businesses

Checklist for Retail IT Security:

- POS systems updated
- antivirus protection installed
- strong passwords used
- MFA enabled
- guest Wi-Fi separated
- payment terminals secured

Retail Shop Technology Maintenance Checklist

- Review Software Updates
- Perform Backup Testing
- Test Hardware
- Check Users' Access
- Monitor the Internet Connection to the Retail Shop

New Store IT Setup Checklist

- Install an Internet Connection with a High Level of Reliability
- Set Up the POS System
- Provide Secure Payment Systems
- Provide Secure Wi-Fi
- Set Up CCTV
- Create Backups for the POS System

FAQs

1. **Do hackers target small retail establishments?**

Yes. Smaller-sized businesses are usually chosen as targets as hackers believe they have weaker security safeguards in place than larger organisations.

2. **How secure are today’s point of sale (POS) systems?**

When properly maintained and updated, today's systems can be considered secure.

3. **When should a retailer update their systems?**

When vendors provide a critical security or stability update.

4. **Is it safe for a retailer to use cloud-based software?**

Cloud providers tend to have reputable levels of security; however, it is important for businesses to carefully manage their access to and/or configuration of their cloud software.

5. What type of IT support should a retail store use?

Retailers who have traditional IT support typically have access to reliable IT support to assist with routine maintenance, security monitoring and/or to troubleshoot any technical problems.

About This Guide

This document was created by the **Computer Support Centre** to provide assistance for UK-based retail businesses on technology's role in day-to-day operation of a shop.

Small independent shops and small retail chains rely heavily upon IT systems such as point of sale (POS) systems, debit/credit card processing terminals, stock management software, and store-wide wireless networks. The intent of this document is to describe the best practices for IT in a simple and easy-to-understand manner so that shop owners, retail managers, and operating personnel will be able to provide better management of their IT resources.

The purpose of this document is to provide retail operators with a simple guide to IT best practices that can assist them in improving their security, reliability, and efficiency, while also ensuring that customer data is maintained securely and that retail operations operate smoothly.

If you learn more about **Computer Support Centre**, our services, and our approach, please visit our official website:
 https://computersupportcentre.com

Conclusion

Today, retail businesses rely heavily on technology to operate smoothly, therefore, having an effective IT infrastructure is vital. To aid in providing quick service to customers, retail stores use technology for everything including point of sale (POS) systems, payment terminals, and managing inventory.

Unfortunately, if technology is not managed properly, retailers may experience interruptions to their operations, failures with their payments, and present themselves with security risks as well. Shopping retailers can take steps to minimise these risks by following best practices of using information technology (IT), such as securing their POS systems, separating guest Wi-Fi from their internal networks, keeping software current, and properly managing employee access.

Retailers who utilise best practices for management of their IT systems simultaneously create a more efficient, reliable, and secure environment that allows for business growth and an improved customer experience over time.