

## Module 2

# How to Inventory Your Devices, Apps, & Accounts

implemented in India by



with support from 

Training Module developed under the project **APAC Cybersecurity Fund**

This training module is designed to provide general information and guidance on cybersecurity best practices. While every effort has been made to ensure the accuracy and relevance of the content, the information provided is for educational purposes only and does not constitute professional advice or an exhaustive cybersecurity strategy. By participating in this training, you acknowledge and accept that the information is provided "as is," without any guarantees or warranties of any kind, express or implied. For tailored cybersecurity solutions, please consult with certified experts.

Organized by **The Asia Foundation**

Implemented in India by **The Foundation for MSME Clusters**

Supported by **Google.org**



Module also available in Hindi, Marathi, Punjabi, Kannada and Telugu

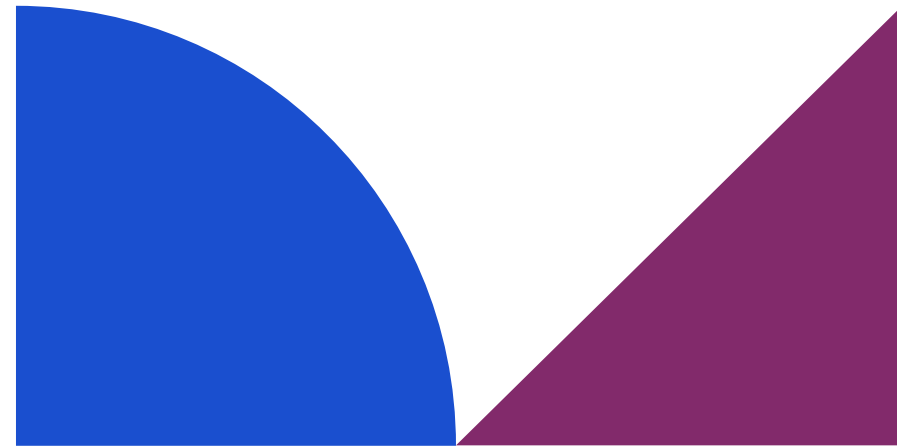
Module developed by **Global Cyber Alliance & CyberPeace Foundation**

Module designed by **Chowdhury, Basu & Ray**

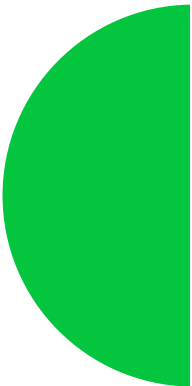
Version 1.0

December, 2024

## Module 2



# How to Inventory Your Devices, Apps, and Accounts



Taking an inventory of your technology assets is a critical first step to protect your organization from cyberattacks. After all, you can't protect what you don't know you have. Knowing what hardware and software is used across your business allows you to maintain control and ensure only authorized, fully supported hardware and software is in use. This will minimize risk introduced by forgotten, unsupported, end-of-life, or unauthorized items because they can more quickly be identified, updated, or removed. Keeping your inventory up to date is critical to ensure ongoing security.

# What We Will Talk About

- 1 HOW DEVICES, APPLICATIONS & ACCOUNTS IMPACT SECURITY
- 2 WHY INVENTORY YOUR DEVICES, APPS & ACCOUNTS?
- 3 KNOW WHAT YOU HAVE CHECKLIST
- 4 INVENTORY TRACKER



How to Inventory Your Devices, Apps, and Accounts

## How Devices, Applications & Accounts Impact Security

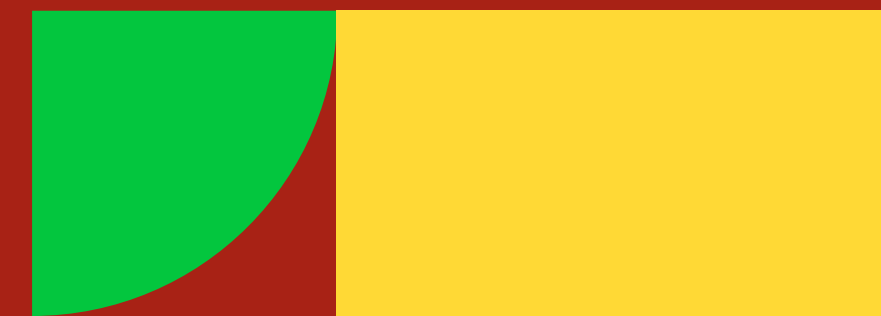
Have you ever taken a moment to really think about the extent you rely on technology in your life?

Knowing what you have is the first step to understanding your risk and better protecting your business.



# Pause to consider a few specifics:

- ✓ How many devices do you own or use each day (mobile, tablet, laptop, desktop, hotspot, etc.)?
- ✓ How many applications are installed on each of those devices?
- ✓ What software and hardware tools do you use to run your business?
- ✓ How many dozens of online accounts do you have?
- ✓ Who has access to those devices and accounts?





## How to Inventory Your Devices, Apps, and Accounts

With each new device, application, or account you add - and each new person having access to those devices and accounts - your security risk increases.

Each additional device, app, or account used in a business increases the "**attack surface**," or the number of entry points attackers can exploit. Devices, applications, and accounts often hold sensitive business and customer data, from payment details to internal communications.

Any unsecured or undocumented asset poses a risk if it's not monitored for updates, access control, and potential vulnerabilities.



**THREAT!**



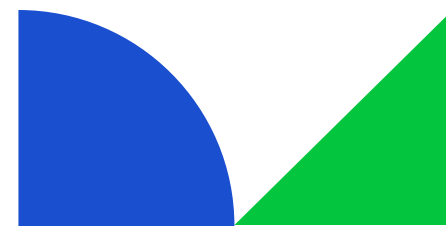
## How to Inventory Your Devices, Apps, and Accounts

**IBM's 2023 Cost of a Data Breach report identifies compromised credentials as one of the most common initial attack methods, accounting for nearly 20% of breaches.**

It is important to think about the security implications whenever you make any changes. Tools are available to help with this, to ensure you can take advantage of technological advancements while minimizing the cyber risk to your business.

Over the next few lessons, we will walk you through taking an inventory. When you understand your IT environment and threat landscape (often referred to as your 'security posture'), you'll know where to implement changes that will make your business safer. It's easier than you think.

Let's get started!



# Why Inventory Your Devices, Apps & Accounts?

Taking an inventory of your technology assets is a critical first step to protect your organization from cyberattacks. After all, you can't protect what you don't know you have. **In India, nearly 45% of cyber incidents in MSMEs result from unsecured or undocumented assets.**

Knowing what hardware and software is used across your business allows you to maintain control and ensure only authorized, fully supported hardware and software is in use. This will minimize risk introduced by forgotten, unsupported, end-of-life, or unauthorized items because they can more quickly be identified, updated, or removed. Keeping your inventory up to date is critical to ensure ongoing security. In India, nearly 45% of cyber incidents in MSMEs result from unsecured or undocumented assets.



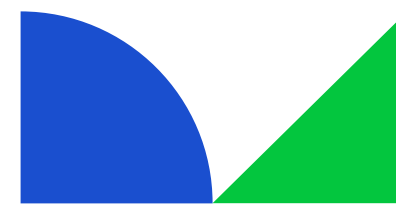


## How to Inventory Your Devices, Apps, and Accounts

When you are thinking about devices you have, **don't forget to consider IoT:**

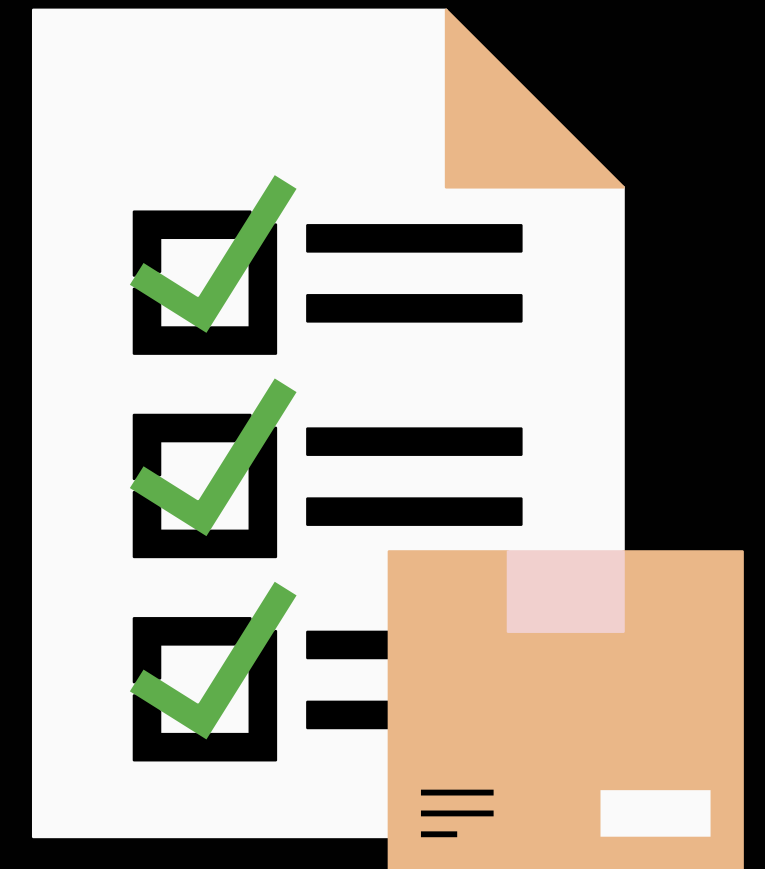
the Internet of Things refers to physical devices that are connected to the Internet and can be controlled and monitored remotely. Examples of IoT devices you may be using in your business include smart security systems, smart thermostats, locks, and remote cameras. If these devices lack security patches or are used across unsecured networks, they can be hacked remotely, potentially exposing business and customer data.

In India, cyber incidents involving IoT devices increased by over 100% between 2022 and 2023, highlighting the urgent need for securing such assets (CERT-In report, 2023).



# **Creating and maintaining a comprehensive inventory tracker for your MSME helps in:**

- Ensuring compliance with cybersecurity regulations and data management standards.
- Preventing unauthorised access.
- Spending intentionally and mindfully after careful regular asset evaluation. MSMEs can save an estimated 15-20% on IT-related costs, as they avoid redundant purchases or licenses.
- Save on tax breaks.
- Increase resilience to cyber threats through timely interventions.
- Simplify incident response protocols, augment cybersecurity SoPs.





## How to Inventory Your Devices, Apps, and Accounts

**Good cyber hygiene is a continuous process which should be built into your existing workflows and workplace habits.**

It is a simple but incredibly effective way to protect your business from cyber threats. Better still, good cyber hygiene isn't costly!

In the next lesson, you'll download a free checklist you can use to help you get started taking your inventory!



How to Inventory Your Devices, Apps, and Accounts

**What types of devices, apps or accounts do you think are most vulnerable in your network?**

**Share with us your thoughts.**

**Interactive  
Session**

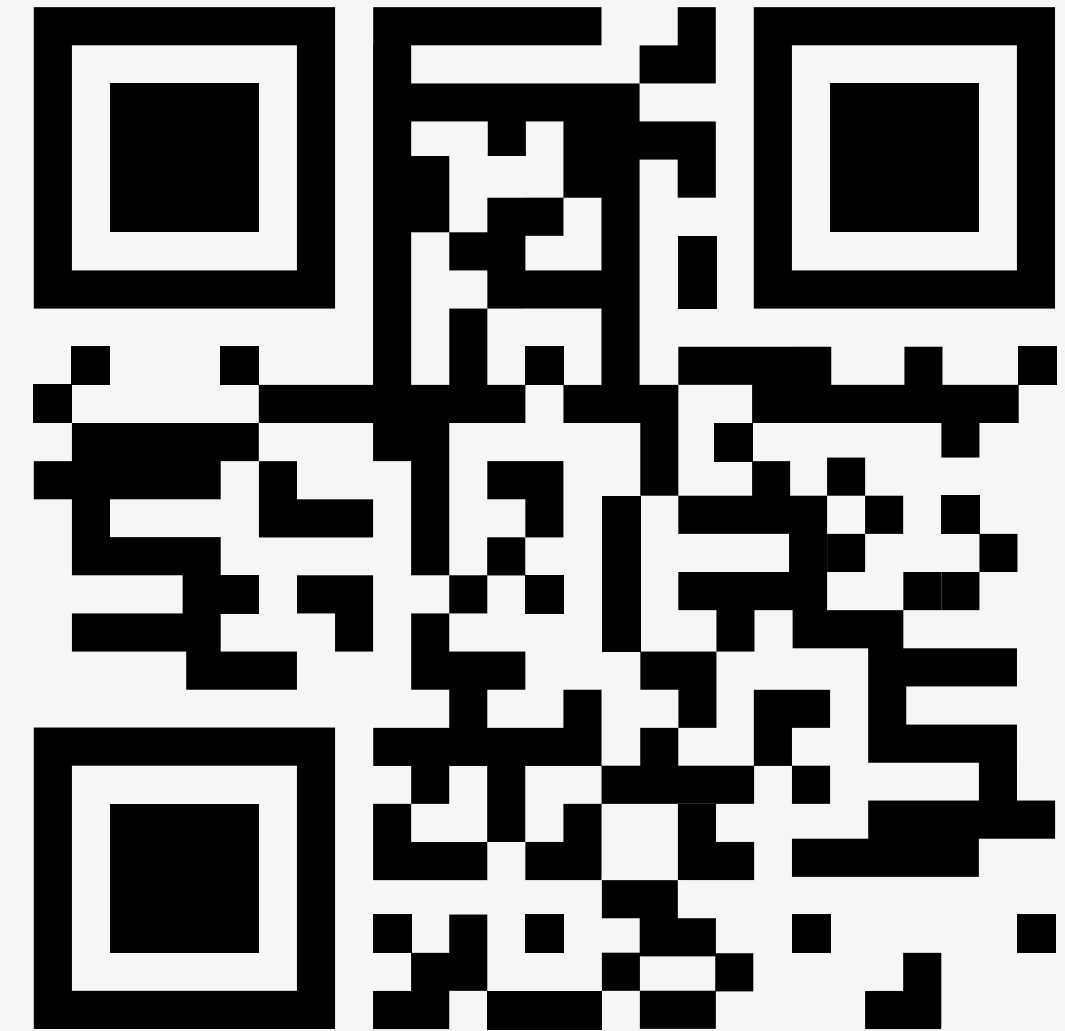




# Know what you have checklist

MSMEs must implement an inventory checklist that logs each device, application, and account, along with details like last update, location, and assigned user. This makes it easier to track and secure assets and also trace and plug leaks.

**Download this Inventory Tracker** to help you record, track, and manage all hardware (mobile, tablet, laptop, desktop, hotspot, etc.), software, applications, and assets on your network or used to support your business operations.



Scan using your phone to  
download the inventory tracker



# How to Inventory Your Devices, Apps, and Accounts

Here are the assets you must incorporate into your inventory tracking checklist:

## Devices & Hardware

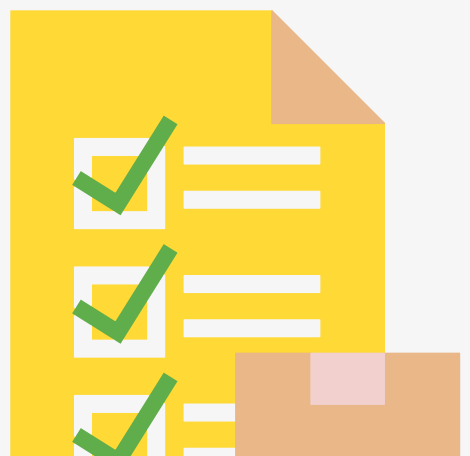
- Laptops
- Desktops
- Mobile
- Phones
- Tablets Used For Business Purposes

## Software

- Operating Systems
- Antivirus & Other Protection Software Subscriptions
- Productivity Software (E.G., Microsoft Office, Google Workspace)
- CRMS
- Accounting Software
- Payment Software, etc.

## Hardware

- Mpos Systems
- Routers And Switches
- Modems
- External Hard Drives And Usbs
- Cables And Adapters
- Ups
- Archival Tapes
- Fax Machines
- Electrical And Electronic Infrastructure





# How to Inventory Your Devices, Apps, and Accounts

Here are the assets you must incorporate into your inventory tracking checklist:

## Applications

- Any and all apps used for essential business functions, such as email, accounting, and customer management.

## Online Accounts

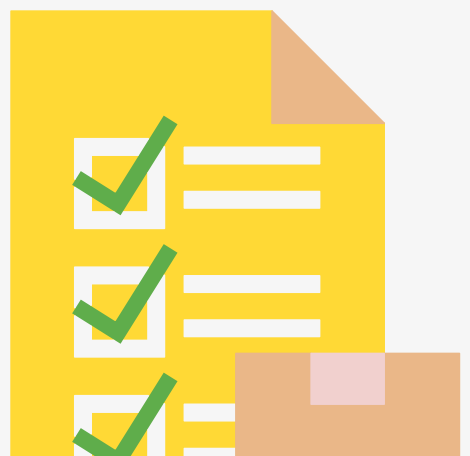
- Email Accounts
- Social Media Accounts
- Payment Processors
- Cloud Storage Accounts
- Organizational Team Channels Like Slack
- Others

## IoT Assets

- Smart Cameras
- Printers
- Sensors
- Others

## Access Controls & Logs

- Who Has Access To Which Devices, Apps, And Account Logs Of Usage  
Logs of Access Changes



## How to Inventory Your Devices, Apps, and Accounts

Taking an inventory of all of these things may sound overwhelming as a busy business owner. But it takes less time than you think, is well worth your effort, and is just as important for protecting your business as having insurance or a good accountant.

The shift to remote work has driven up the cost of breaches by nearly 15%, with personal devices often being used over unsecured connections. For MSMEs relying on remote work, implementing secure access protocols, even for personal devices, is crucial for reducing potential breach costs.

If you don't have time to take your inventory right now, **we recommend putting time aside on your calendar to do it a little bit at a time.** For example, inventory devices and hardware first, do software another day, applications next, and then online accounts. Don't forget to include information about who has access to each account.





## How to Inventory Your Devices, Apps, and Accounts



OR



Google Sheets

This inventory will be a useful tool for many reasons in your business, but remember to update it every time you make any changes

**You can set up a tracker free of cost in MS Excel or Google Sheets.**

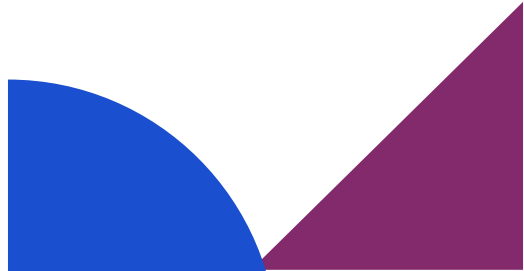
Include columns for device name, type, serial number/ ID, purpose, department, assigned user, date of acquisition, security software, location, and last update.

## How to Inventory Your Devices, Apps, and Accounts

Here's a quick list of things you can do **to make the most of your inventory tracker**:

As you develop strong cyber hygiene habits, here is **a quick checklist** of common mistakes to avoid:

- **Update Regularly:** Conduct quarterly inventory audits to capture any changes, including new devices or applications.
- **Limit Access to Tracker:** Restrict access to the inventory tracker to prevent unauthorized changes or viewing of sensitive asset data.
- **Create Backup Copies:** Store backup copies of inventory files offline in case of data loss or cyberattacks.
- **Automate inventory updates** using tools that sync with your network, providing real-time visibility into assets.
- **Regularly review and update device policies** as employees bring new devices or software into the workplace.
- **Add a Summary Dashboard:** Create a quick overview on a separate sheet, showing key stats using pivot tables.
- **Use IoT-specific security settings** to limit vulnerabilities, such as limiting network access and regularly updating firmware.
- **Don't forget to keep an inventory of any cloud storage options you're using!**





How to Inventory Your Devices, Apps, and Accounts

# Any questions or thoughts?

Share with us your queries or thoughts before we proceed to Module 3

Q&A  
Session



# Thank you for your attention!

For further assistance you can also reach out to the CyberPeace Foundation at [helpline@cyberpeace.net](mailto:helpline@cyberpeace.net) or on WhatsApp at +91 957-00-000-66

Training Module developed under the project **APAC Cybersecurity Fund**

implemented in India by



with support from 