APAC Cybersecurity Fund

The Asia Foundation

Module 1

Understanding Cyber Risk for MSMEs in India

implemented in India by

with support from Google.org

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 1

Understanding Cyber Risk for MSMEs in India

Cyber-attacks target micro, small, and medium-sized enterprises (MSMEs) just as often as large ones, but MSMEs don’t often have teams or resources dedicated to actively protect against these attacks.

This course will teach you the basic protection measures your business against cybersecurity threats with the limited resources most MSMEs have at their disposal. It will show you how to reduce your cybersecurity risk level in practical ways that don’t require a lot of time, money, or expertise.

What We Will Talk About

1. CYBER RISK FOR MSMES: WHY IS IT SO IMPORTANT?
2. WHERE DOES CYBER RISK COME FROM?
3. FUNDAMENTALS OF CYBER HYGIENE
4. NEXT STEPS

Cyber Risk for MSMEs: Why is it so important?

‘Cyber risk’ indicates the probability that your business will suffer a loss. It can take many forms.

This can include financial loss, disruption to business operations through a hacked website or social media account, loss of critical data or personal information of employees or customers, as well as reputational damage. Protecting your business and managing your cyber risk needs to be part of your overall business operations and planning.

Cybersecurity for MSMEs helps to:

- Protect sensitive business information.
- Protect customer data.
- Build a trustworthy brand.
- Protect stakeholder interests.
- Avoid downtime
- Ensure business continuity.
- Achieve supply chain stability.
- Inspire partnerships.
- Protect financial information.
- Protect intellectual property.

Here’s why cybersecurity for MSMEs in India is relevant:

MSMEs in India represent 30% of GDP. According to the Ministry of MSME (2023), nearly 60% of Indian MSMEs have experienced cyber incidents but lack comprehensive cyber defenses. India has seen a 300% increase in cybercrimes against small businesses since 2021. -National Cyber Security Coordinator.

According to the DSCI, 43% of cyberattacks in India target small businesses. MSMEs face the same threats as large corporations but have fewer defenses. The urgency is heightened as India promotes digital adoption under the Digital India initiative. With MSMEs increasingly establishing online presences and integrating mobile-first technologies, they become primary targets for attackers who exploit limited cybersecurity frameworks.

Where does cyber risk come from?

There are 2 classifications of cyber risks:

- on the basis of **Origin** and
- on the basis of **Intent**

Cyber risk on basis of

Origin

- **Internal Risks**: Employee errors, unsecure Wi-Fi, weak passwords.
- **External Risks**: Phishing, ransomware, and malware attacks from third-party actors.

Cyber risk on basis of

Intent

- **Deliberate:** Ransomware, phishing.
- **Incidental/Accidental:** Employee accidentally opens a phishing email, uses a public Wi-Fi, has weak passwords. Incidental threats include cases where MSMEs that are dragged into a cyber incident that is actually targeting a larger corporation or as a result of some other incident like an unrelated data breach or a power outage creating system vulnerabilities.

Understanding Cyber Risk for MSMEs in India

When we talk about cyber crime, it is essential to remember that cyber criminals are organized. Today, most threats come from organized attempts to steal data to sell for financial gain and utilize a centrally controlled network of collaborators, each performing a specific function, creating a sophisticated hierarchy that is easily scalable and repeatable.

Cyber criminals will take advantage of any opportunity to exploit world events, regional disasters, and individual weaknesses for their own purposes and gain.

Internal threats can also be deliberate, originating from within the organization, often by employees or former employees. Malicious insiders are different from negligent insiders.

The business of cyberattacks:

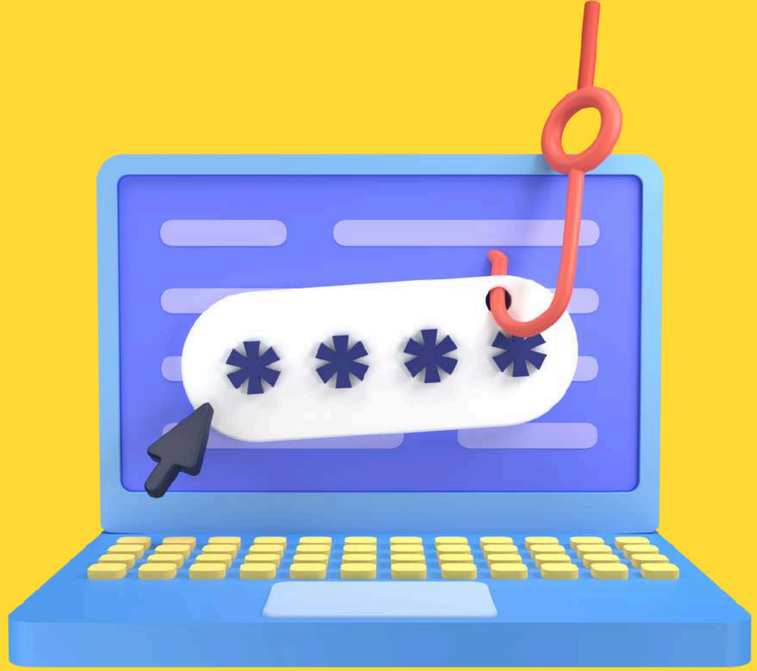
Cybercriminals monetize successful attacks either by stealing data and directly selling it or by holding the data hostage and demanding ransoms (this approach is known as a ransomware attack).

Ransoms are an especially attractive revenue stream for hackers because this approach doesn't require finding a buyer for the stolen data in the underground market. Ransoms are typically paid in more difficult to trace bitcoin, which most companies don't have easy access to.

Cybercrime Market Players:

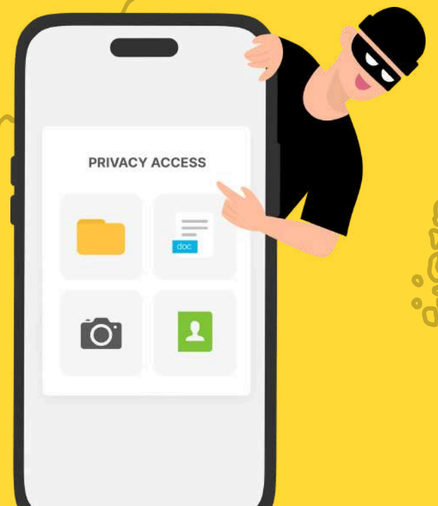
- **Sole Traders/Lone Wolves:** Operate alone or with a small handful of individuals to create and sell cyberattack products.
- **Organized Crime Groups:** Coordinated networks of highly sophisticated hackers, developers, and organizations who exploit and monetize the data they've stolen.
- **Marketplace:** Platforms for individuals and groups to buy and sell cyberattack products or services.
- **Supply Chain:** Network of creators, developers, and suppliers for cyberattack products and services.

Cyber criminals may not be targeting you or your business specifically!



- **Supply chain:** You may be targeted because they see your business as a potential route into a higher profile customer or partner of yours.
- **Outdated or pirated systems/software:** You may fall victim to an attack because of the systems or software you happen to be running.
- **User error:** You may fall victim to an attack because you or a member of your staff acted on a phishing email, unwittingly visited a malicious website, or accessed accounts via insecure Wi-Fi network.

Why MSMEs in India are prime targets?



As per Statista's report of Global Internet Access, India is a mobile-first nation, with over 1.05 billion internet users primarily accessing the internet through smartphones.

MSMEs primarily rely on mobile phones and digital tools for business operations. 95% of MSME transactions are mobile-based, making them prime targets for mobile-specific threats.

MSMEs are attractive targets due to lower security investments and high-value financial transactions. There are many reasons why your business could be a victim of cybercrime — understanding and reducing risks wherever you can make good business sense.

Interactive Session

Have you ever faced any cyber-threat ?

Share with us your experience

Understanding Cyber Risk for MSMEs in India

Managing Cyber Risk

With the increasing interconnectivity of all of our systems and devices, as well as changes in how we conduct business, security weak spots and vulnerabilities are growing exponentially.

Most MSMEs do not have the time or expertise to effectively address these on their own.

Challenges faced by MSMEs

MSMEs face some unique challenges when it comes to cybersecurity, owing to their scale of operations and the resources at their disposal. These include:

- Limited budgets.
- Cannot hire or contract specialized IT / cybersecurity personnel.
- Old devices.
- Legacy infrastructure.
- Outdated or pirated software.
- Lack of tech-savvy.

Implementing the most basic cyber hygiene practices can **prevent up to 86% of the most basic cyber-attacks**. Keep in mind that no matter what type of device you are using to support your business (mobile phone, tablet, laptop, and/or desktop) these same cyber hygiene steps apply.

Things you may be concerned about:

- It seems too hard.
- I don't have the time.
- I don't have the funds to pay someone to help me.
- I don't have the funds to buy tools to protect my business.

You are not alone! These are common and legitimate concerns. But this series of mini-courses is designed to give you a basic understanding of the steps you can take and the resources available to help you

Fundamentals of Cyber Hygeine

Leadership: Lead by example and educate your staff, volunteers, or family members who might also share your devices on the basics you learn here.

Know what you have: Keep an inventory of hardware and software that you use for your business. Deactivate devices (mobile, tablet, laptop, desktop, hotspots, etc.) or accounts you no longer use.

Backups: Consistently backup your data and keep multiple copies off-premise and with a secure cloud solution.

Software updates: Do them right away and automate all the ones that you can. Software systems that are not up-to-date with the latest security patches are one of the biggest risk factors to your business.

Passwords and tools to protect them: Create unique and strong passwords for each account. Use two-factor authentication and password managers for added security.

Access control: Not everyone needs access to everything or the same privileges. Limit users and permissions to only what they need. This includes the ability to download **new software or apps.**

Remember that cybersecurity is for ALL members in an organization and not limited to any one department or team. If every person in the organization is aware of good cyber hygiene, there are fewer opportunities for cybercriminals to gain unauthorized access.

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

- Don’t use default or easily guessable passwords, and avoid password reuse across accounts.
- Don’t leave systems and software unpatched, as vulnerabilities can be exploited by attackers.
- Don’t open untrusted or suspicious emails, attachments, or links, as they may contain malware.
- Don’t store sensitive data or passwords in plain text or unencrypted formats.
- Don’t grant excessive privileges or access rights to users beyond what is necessary.
- Don’t neglect physical security measures, such as access controls and secure disposal of sensitive data.
- Don’t disable or bypass security controls, such as firewalls, antivirus software, or IPS/IDS systems.
- Don’t connect untrusted or unauthorized devices to your network.
- Don’t share sensitive information or credentials over unsecured channels or public networks.
- Don't ignore security alerts, warnings, or suspicious activities, and promptly investigate and respond.

Before we jump into the courses, here's a **quick action plan** to keep handy in case you're ever hit by a cyber attack in India:

- Call the national Indian Cyber Crime Helpline at 1930.
- Report to CERT-In: Notify the relevant authorities for mandatory reporting. Report on the cybercrime.gov.in portal
- Lodge a complaint at your local police station / cyber cell.
- Identify the incident: Determine if it's a data breach, ransomware, or phishing attack.
- Contain the damage: Disconnect affected systems to prevent spread.
- Notify stakeholders: Maintain transparency to uphold trust with customers, funders-donors, partners, service providers and the relevant authorities.
- Prepare for larger communication in the event of media involvement. Choose if you want to release a social media statement at every stage.
- Restore from backups: Ensure regular backups to minimize operational downtime.
- Review and improve cybersecurity measures: Learn from the incident to strengthen defenses.
- Ask an external expert or auditor to gauge your response and recovery efforts.

Q&A Session

Any questions or thoughts?

Share with us your queries or thoughts before we proceed to Module 2

APAC Cybersecurity Fund

The Asia Foundation

Thank you for your attention!

For further assistance you can also reach out to the CyberPeace Foundation at 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 Foundation for MSME Clusters (FMC)

with support from Google.org

APAC Cybersecurity Fund

The Asia Foundation

Module 2

How to Inventory Your Devices, Apps, & Accounts

implemented in India by Foundation for MSME Clusters (FMC)

with support from Google.org

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?

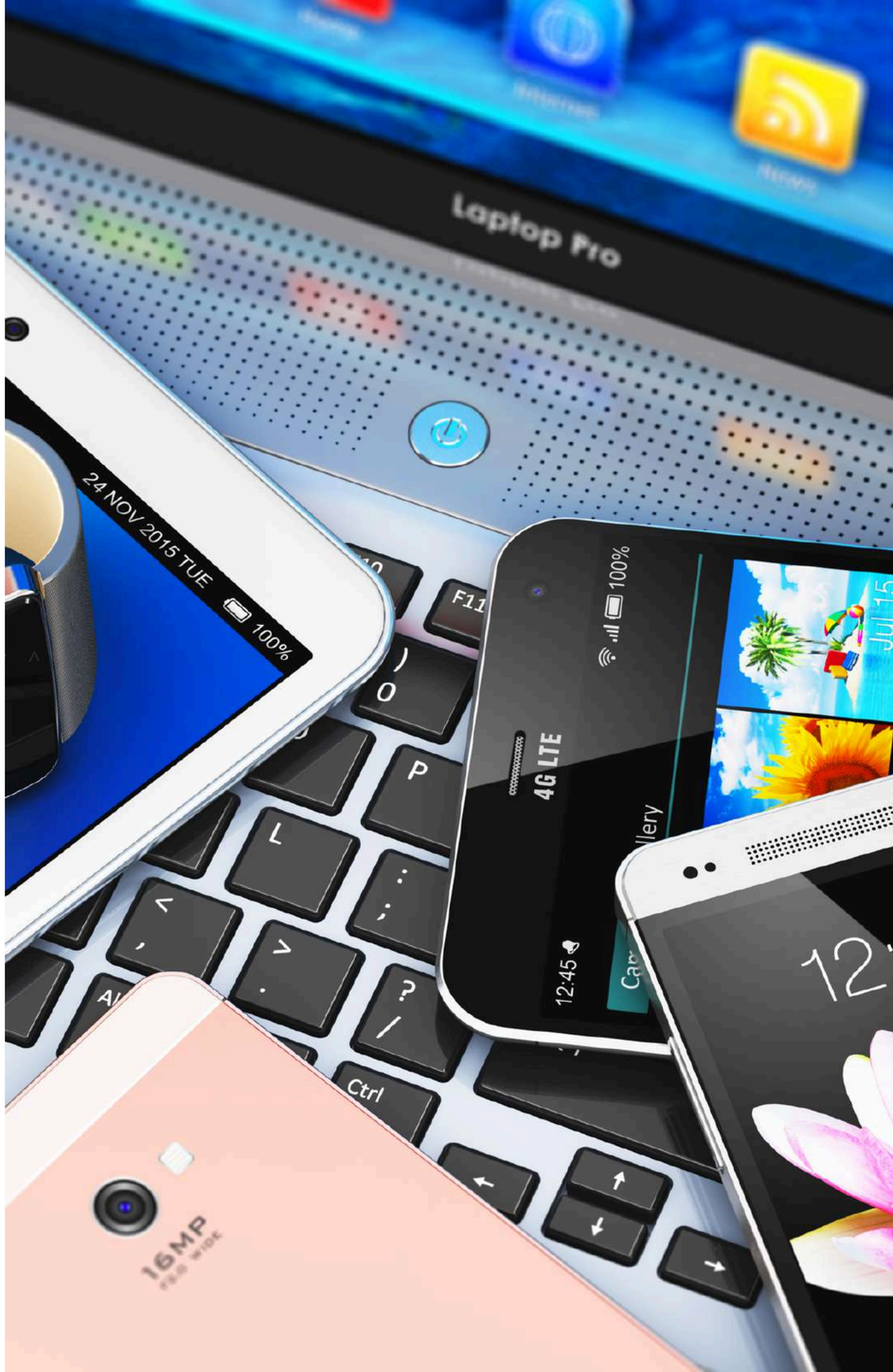
3 KNOW WHAT YOU HAVE CHECKLIST

4 INVENTORY TRACKER

How 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.

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

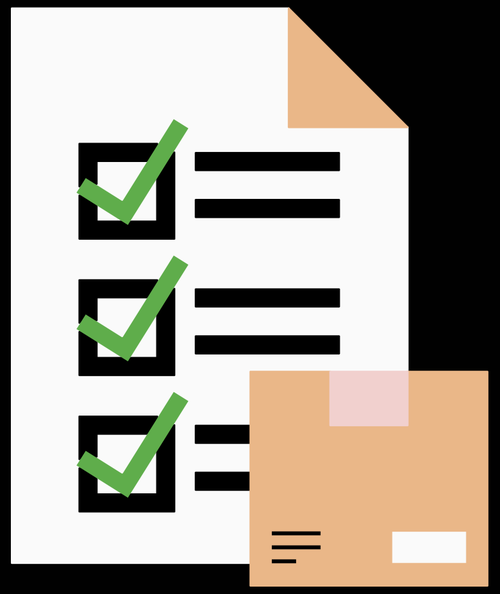
When you are thinking about devices you have, **don’t forget to consider IoT:**

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.



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!

Interactive Session

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

Share with us your thoughts.

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

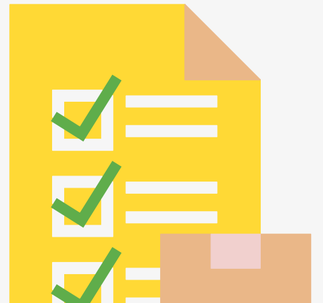
- Laptops
- Desktops
- Mobile
- Phones
- Tablets Used For Business Purposes

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

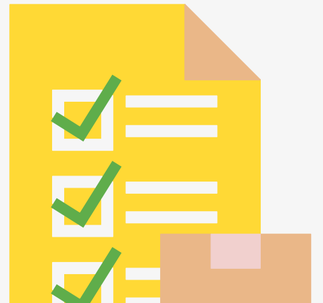
- Email Accounts
- Social Media Accounts
- Payment Processors
- Cloud Storage Accounts
- Organizational Team Channels Like Slack
- Others

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



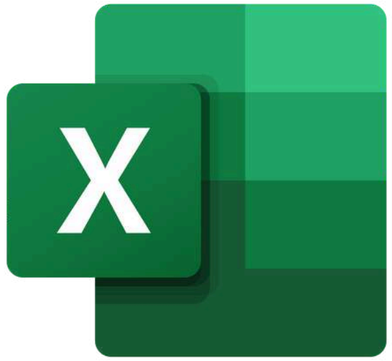
How to Inventory Your Devices, Apps, and Accounts

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

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!

Q&A Session

Any questions or thoughts?

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

APAC Cybersecurity Fund

The Asia Foundation

Thank you for your attention!

For further assistance you can also reach out to the CyberPeace Foundation at 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 Foundation for MSME Clusters (FMC)

with support from Google.org

APAC Cybersecurity Fund

The Asia Foundation

Module 3

Software Updates and Business Security

implemented in India by

Foundation for MSME Clusters (FMC)

with support from Google.org

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 3

Software Updates and Business Security

Manufacturers and software developers regularly update their applications and operating systems to address newly discovered weaknesses or vulnerabilities in their products. These updates will be available for all types of devices (mobile, tablet, laptop, desktop, hotspot, etc.) and apps. Be sure to pay attention no matter what type of devices you use.

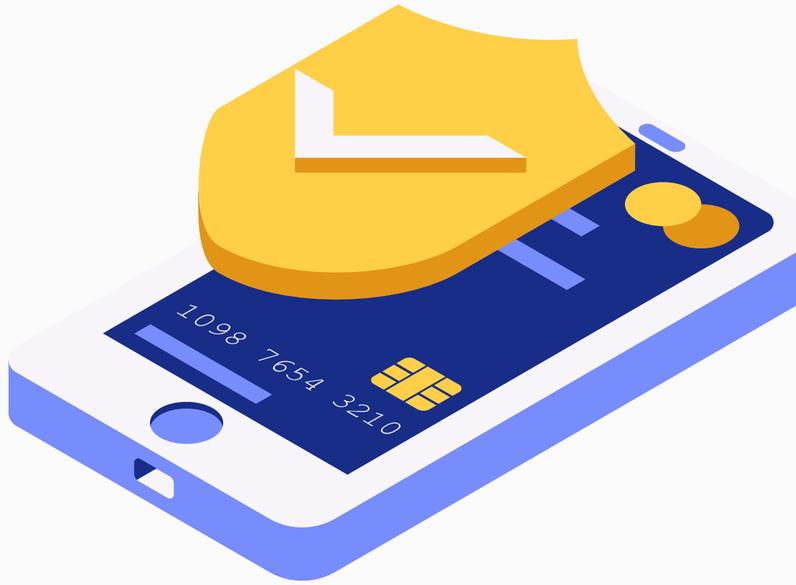
These fixes are referred to as software updates or patches and the process is known as patching.

What We Will Talk About

1. SOFTWARE PATCHING IMPROVES YOUR SECURITY.
2. DO SECURITY PATCHES EVER STOP BEING MADE?
3. IOT (INTERNET OF THINGS) DEVICES
4. CHECKLIST

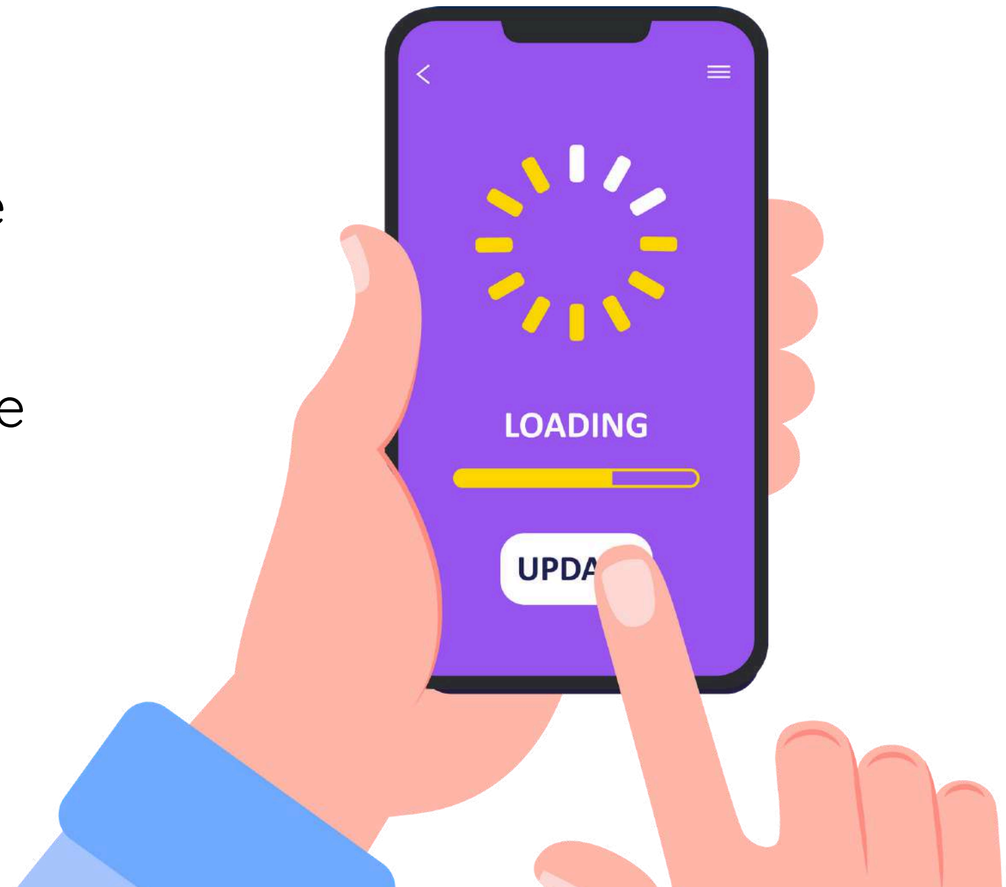
Software patching improves your security.

- Remember, cyber criminals are constantly looking for ways to gain access to systems, accounts, and data.
- A way they do this is by finding a weakness in a configuration or code they can replicate across the entire user base and exploit it to their advantage.
- Patching is critical to your security and should be done as soon as possible.
- It is absolutely critical for patches to be applied quickly and automatically whenever possible to protect your personal and professional data from being compromised.



Here’s a quick snapshot of some other reasons why you need to prioritise your software patches and updates:

- Compliance Issues: Legacy software may not meet current regulatory standards.
- Incompatibility with Modern Systems: Legacy software may not integrate with newer systems.
- Decreased Efficiency and Performance: Older software may be slower and less stable.
- Lack of Vendor Support: Legacy software may no longer receive vendor support.



Some real-world example of how users failing to download a readily-available security patch had devastating effects.

- **IRCTC Breach (2018):** Hackers exploited vulnerabilities in the IRCTC (Indian Railway Catering and Tourism Corporation) booking platform, which was using outdated security measures. Exposed the information of around 200,000 passengers for two years. The vulnerability allowed users to be redirected to a third-party insurer, which exposed their information.

- **Aadhaar Data Breach (2018):** The Aadhaar system, which houses biometric and personal data of over 1.3 billion Indians, suffered data breaches due to insufficient patch management.

- **JustDial Data Breach (2019) :** In 2019, JustDial, a major Indian local search engine, suffered a data breach that exposed over 100 million customer records, including names, phone numbers, email addresses, and physical addresses. The breach occurred due to a vulnerability in their software that allowed unauthorized access to their database. The breach was reportedly linked to an insecure API and inadequate security measures.

Do Security Patches Ever Stop Being Made?

“End of Life” and Software Updates

- All devices and operating systems have an “end of life” date after which they are no longer maintained. After this date, technical support ceases and no further patches are released.

- Using these devices and systems after their "end of life" becomes an immediate and ongoing risk for any newly discovered vulnerabilities. This stop of patching can also happen if a manufacturer ceases trading and no one takes on the development of its product set.

IoT (Internet of Things) Devices

The dramatic growth of Internet of Things (IoT) devices has exponentially increased potential access points for attackers. Many of the IoT devices used on a daily basis have very limited security features or no patching capabilities. This means if a flaw does exist, your network would be open to attack until the device is physically removed or proper security measures are implemented.

IoT devices often face patching limitations due to:

- Device Manufacturer Support: Many IoT manufacturers do not provide ongoing updates for older devices.
- Lack of Standardization: IoT devices often operate on proprietary firmware, which makes regular updates challenging.
- Many IoT devices lack automatic update features, making them vulnerable to attacks. In India, CCTV cameras, smart printers, and eve POS machines often run on outdated software.

Examples Of Outdated Devices Still Being Used In India

- **Windows XP PCs**: Despite Microsoft officially ending support for Windows XP in April 2014, it is still used in several parts of India, particularly in government offices, small businesses, and educational institutions, mainly due to legacy software dependencies.
- **Windows 7 PCs**: Though Microsoft ended support for Windows 7 in January 2020, many businesses and individuals still use it because of the cost and compatibility issues associated with upgrading. Windows 7 is still prevalent in various MSMEs across India.
- **Old Mobile Phones**: Feature phones, especially those running outdated operating systems like Nokia's Series 40 or earlier versions of the Android OS (such as Gingerbread), are still widely used in rural India due to affordability. These devices don't receive updates and are more vulnerable to security threats.
- **Old POS Terminals**: Many small retailers in India still use legacy POS terminals that run on outdated operating systems (Windows CE, Windows XP). These devices may lack modern security features like encryption and secure transaction protocols.
- **Legacy ATM Machines**: Numerous ATMs across India still run on outdated software and hardware that are vulnerable to security threats. These ATMs often run on old operating systems, such as Windows XP or outdated versions of Windows 7, which may not be receiving security updates anymore.

Software Updates and Business Security

Old applications that are no longer in use and older or outdated equipment (mobile, tablet, laptop, desktop, hotspot, etc.) should be removed or deactivated as quickly as possible to avoid these security risks. These should ideally have been identified and removed/updated while completing your inventory.

Stop using and replace any unsupported systems that have not been upgraded/replaced:

Some systems that have gone end of life that aren't actively being supported/protected:

- **Windows 7** went end of life in **January 2020**
- **Windows XP** went end of life in **April 2014**
- **Windows 10** will be at its end of life **October 14, 2025**

Examples Of Outdated Software Solutions Still Being Used In India

- **Microsoft Office 2007:** Microsoft Office 2007, while still in use in many businesses, no longer receives official support or security patches from Microsoft since 2017. It lacks modern features, compatibility with newer file formats, and suffers from potential vulnerabilities.

- **Outdated Accounting Software**: Many MSMEs in India still use legacy accounting software like Tally ERP 9 (pre-2020 version) and Busy Accounting Software (older versions), which may not be receiving updates or patches, leaving them open to security risks.

- **Adobe Flash Player**: Adobe Flash Player was officially discontinued by Adobe in December 2020. Despite this, some businesses in India continue to use legacy systems or software that rely on Flash for web functionality, exposing themselves to potential security risks as no further updates or support are available.

- **Older ERP Systems**: Many companies continue to use outdated versions of SAP ERP (pre-2015 versions) or Oracle ERP. These older Enterprise Resource Planning systems are prone to vulnerabilities, especially if they haven’t been patched or upgraded in years.

- **Antivirus Software:** Legacy antivirus solutions like Norton 2008-2010 or McAfee 2009-2012 are still being used in many Indian businesses, especially by small businesses and home users. These outdated solutions no longer offer adequate protection against modern cyber threats.

Examples Of Outdated OS Solutions Still Being Used In India

- **Windows Server 2008/2003:** Windows Server 2008 and 2003 are still being used in some Indian organizations. However, both have reached their end-of-life dates (2008 in January 2020 and 2003 in July 2015), and their lack of updates leaves them exposed to cyberattacks.

- **Microsoft Internet Explorer (pre-2015 versions):** Internet Explorer versions prior to 2015 (especially versions 8-10) are still in use, despite no longer being supported by Microsoft. Many businesses in India continue to use legacy applications that require Internet Explorer, making them vulnerable to security breaches.

- **Windows Vista:** Though obsolete, some businesses and government institutions in India continue to use Windows Vista due to software compatibility issues. It stopped receiving support in 2017, leaving systems open to unpatched vulnerabilities.

Automatic Updates and Checklist

Most devices and applications can be set up to automatically update which will make it easier to protect your business. When you maintain security updates, you boost your digital immunity against threats such as viruses, spyware, and more.

Just as we discussed creating an inventory for all our devices in the previous module, we must also maintain an inventory of the patches needed and updated for each of the said devices. A device-wise check involves evaluating every device within the organization to ensure all software is up to date, secure, and operating efficiently. This should be done regularly as part of your business's cybersecurity strategy.

Software Updates and Business Security

- **PCs & Laptops:** These are common targets for ransomware and malware attacks. Ensure antivirus software, firewalls, and operating systems are updated.

- **Mobile Devices:** Mobile phones and tablets are increasingly used in business operations, making them attractive targets for hackers. Update mobile operating systems (iOS, Android) and apps regularly to reduce risk.

- **Servers:** Ensure that server operating systems, databases, and application software are updated, as these often hold sensitive customer data.

- **IoT Devices:** Regularly check the firmware and software on IoT devices such as security cameras, smart thermostats, and connected machinery.

Software Updates and Business Security

Use the following checklist to learn how to better protect your business with updates and patches.

- Prioritize Security Patches
- Automate Updates for All Software for All Devices
- Schedule Manual Updates for Systems That Don't Support Automatic Updates
- Maintain an Inventory of Software & Devices
- Conduct Regular Vulnerability Scans
- Test Patches Before Deployment
- Implement Multi-Layered Security
- Ensure Compliance with Local Regulations
- Use Cloud-Based Solutions with Auto-Updates
- Monitor for End-of-Life (EOL) Software & Devices
- Use Middleware or APIs. Plan Gradual Migration to Modern Platforms
- Backup Critical Data Regularly
- Educate Employees on Update & Security Protocols
- Set a Patch Management Schedule
- Review and Update Third-Party Software
- Keep IoT Devices Secure
- Regularly Review Software EOL DatesConduct
- Test Patches Before Deployment
- Backup & Protect Software and System Configurations
- Use Reliable Patch Management Software
- Use Centralised Patch Management Software
- Monitor for Cybersecurity Breaches
- Limit Internet Access for Devices Using Legacy Software
- Consider Virtual Desktop Solutions that Offer Limited Exposure
- Prioritise Patches Based on Severity of the Vulnerabilities They Address
- Do A Criticality Assessment for All Systems to Assign Priority Ratings While Developing an Incident Response Protocol

Q&A Session

Any questions or thoughts?

Share with us your queries or thoughts before we proceed to Module 4

APAC Cybersecurity Fund

The Asia Foundation

Thank you for your attention!

For further assistance you can also reach out to the CyberPeace Foundation at 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 Foundation for MSME Clusters (FMC)

with support from Google.org

APAC Cybersecurity Fund

The Asia Foundation

Module 4

Passwords, Password Management, and Two-Factor Authentication

implemented in India by

with support from Google.org

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 4

What We Will Talk About

Passwords, Password Management, and Two-Factor Authentication

One of the most common ways hackers gain access to your accounts, network, and information is to log in as you.

Hacking passwords is easier than ever. Programs are available that can crack a password in seconds or minutes.

People often reuse the same password, which means once an unauthorized user has gained access to one of your accounts, they've effectively gained access to them all. It is important that you use a unique password for every account to prevent this from happening to you.

1. WHY STRONG PASSWORDS MATTER
2. HOW CRIMINALS GAIN ACCESS TO YOUR PASSWORDS
3. CREATING STRONG PASSWORDS AND PASSPHRASES
4. STRONG PASSWORD CHECKLIST

Strong passwords helps to:

- Protecting your identity
- Financial security
- Protecting your business reputation
- Preventing unauthorised access to your business' social media accounts
- Protecting operations
- Preventing supply chain disruptions

How Criminals Gain Access to Your Passwords:

Once criminals get a password, they can easily sell it on the ‘dark web,’ which is an illicit market on the Internet for buying and selling sensitive data. There are many techniques criminals use to access passwords:

Passwords, Password Management, and Two-Factor Authentication

Password Hacking Methods

Passwords, Password Management, and Two-Factor Authentication

There are many techniques criminals use to access passwords:

- **Social engineering:** Criminals are very skilled at manipulating conversations and using various unexpected ways (a phone call, text message, or social media) to appear legitimate and trick you into revealing your passwords and other personal information. Phishing emails are the most common type of social engineering attack.

- **Manual guessing:** Using personal information like names of sport teams, pet names, or date of birth to guess part of your password. They often get this information from public sources or even from your own social media posts. During the pandemic, attackers exploited default or predictable passwords like "password123" or "admin" on healthcare MSME systems, gaining unauthorized access to sensitive patient data.

- **Credential stuffing:** Once one account has been compromised, they will try the same username/password elsewhere. The Zomato breach (2017) exposed 17 million user records. Stolen credentials were reused in credential stuffing attacks on other platforms where users reused passwords.

- **Credential stuffing:** Once one account has been compromised, they will try the same username/password elsewhere. The Zomato breach (2017) exposed 17 million user records. Stolen credentials were reused in credential stuffing attacks on other platforms where users reused passwords.

Passwords, Password Management, and Two-Factor Authentication

- **Dictionary attack:** A form of brute force attack that uses known dictionary words/phrases or common passwords.
- **Shoulder surfing:** In a public place, or even at your desk, there may be someone watching your activity.
- **OTP Related Scams:** Fake “bank official” calls ask citizens to share OTPs to "validate" accounts, leading to large-scale fraud in UPI transactions. These scams constituted a significant portion of digital payment fraud in 2023.
- **Credential stuffing:** Once one account has been compromised, they will try the same username/password elsewhere. The Zomato breach (2017) exposed 17 million user records. Stolen credentials were reused in credential stuffing attacks on other platforms where users reused passwords.
- **Ransomware/ Malware:** This refers to malicious software that encrypts data (ransomware) or damages systems (malware), demanding a ransom for recovery or exploiting vulnerabilities to steal sensitive information. The WannaCry ransomware attack in 2017 affected Indian MSMEs reliant on outdated Windows systems, causing massive data loss and operational shutdowns.

Passwords, Password Management, and Two-Factor Authentication

- **Keylogging Tools:** Software or hardware tools that record every keystroke made on a device, capturing sensitive information like passwords, account details, and personal data.

- **Credential Theft & Reuse:** Cyber criminals will steal passwords or credentials and then use them across multiple platforms where the victims are likely to have reused the same login credentials. One account breach sets off a chain of breaches. Leaked Aadhaar credentials were reused in multiple fraudulent financial activities, showcasing the dangers of credential reuse across platforms

- **Unsecured Networks & Public Wi-Fi:** Open, unencrypted networks can be targeted to intercept sensitive data and steal potential information. This is especially likely during high-volume traffic/ transactions such as when people use free public Wi-Fi at trade fairs.

- **Exploiting Unpatched Software:** Cyber criminals will often take advantage of known vulnerabilities in outdated or unpatched software to gain unauthorized access to systems or data.

- **Physical Access:** Direct physical access to or possession of devices can allow malicious actors to bypass remote/ digital security protocols.

- **Account Recovery Exploits and Impersonation Scams:** These refer to fraud schemes where attackers use publicly-available or stolen information to exploit account recovery processes and impersonate legitimate users, thereby seeking “help” to “regain lost access” to other people’s accounts.

- **Leveraging Online Marketplaces:** Cybercriminals posing as sellers or customer service representatives on e-commerce platforms can steal login credentials, payment details, or personal information.

Creating Strong Passwords and Passphrases

Once criminals get a password, they can easily sell it on the ‘dark web,’ which is an illicit market on the Internet for buying and selling sensitive data. There are many techniques criminals use to access passwords:

- Use unique passwords or passphrases for each account
- Keep your passwords or passphrases in a safe place (see later lesson on password managers)
- Do NOT use common words such as “password” or “123456” that are easily guessable
- Do NOT use personal information such as your birthday or your pet’s name
- Do NOT share your password unless it is absolutely necessary (see later lesson for examples of when and the best method to minimize the risk)

Creating Passphrases:

A good way to make your password difficult to crack is by combining three random words. This is called a passphrase and will be easier for you to remember than a password with many different characters, numbers, and upper/lowercase letters. It will also be more unpredictable and harder for a criminal to guess or crack.

Tips for creating passphrases:

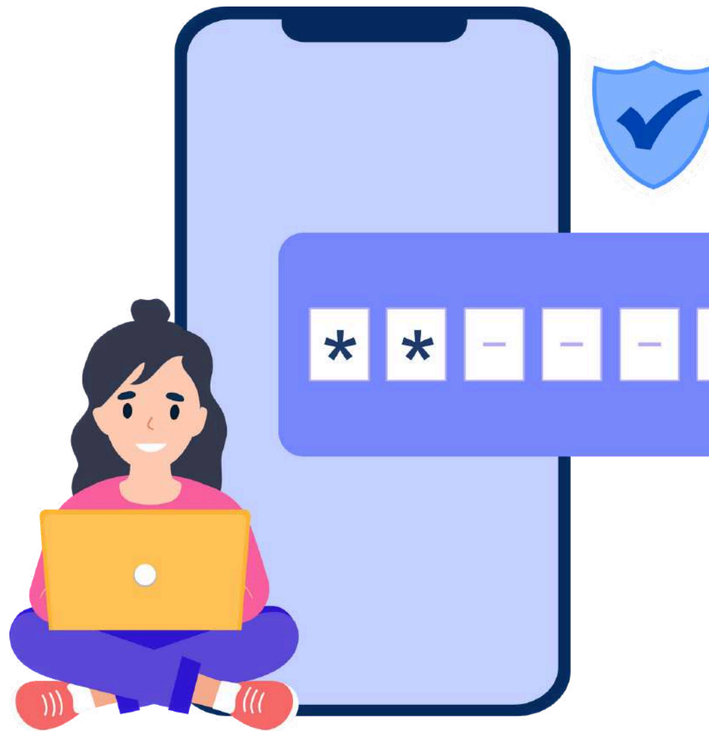
- Choose relatable words
- Avoid predictable famous phrases like “unity in diversity”
- Use your regional identity
- Use your personal interests
- Go for phrases and words that are meaningful to you but hard to guess for others
- Ensure a minimum of three to four words

Creating complex passwords:

A password made up of lowercase and uppercase letters, as well as numbers and special characters, is more complex than a password containing only lowercase letters.

Here are some tips:

- Use a password manager to create and store them for you (see later lesson on password managers)
- Or you can create your own. A good system to use is taking a 3-4 word phrase and combining symbols, numbers, and letters to spell out.
- Example: I love birthday cake = il0v3b1rthd@yc@k3!
- Here are some great examples for the Indian audience: Ganga#Diwali@Namaste or Kerala_Coconut#123 or SpicySamosa@56%



Sharing Account Login:

Sharing of account login information is understandably a very convenient way to save costs as an MSME, however, it brings greater risk to your business. Sharing account login information is never recommended, however, some online platforms commonly used by small enterprises only allow one user login. And that is just not very practical. So let’s talk about safer ways to share that login information.

Top tips:

- Never share the username and password or passphrase in one message such as a single email or single text. If this is intercepted, then someone else will have full access to that account.

- Never share the information if asked by someone else if it is not a conversation you have initiated, especially if you get a request from a phone number you do not recognize, or an email asking you to click on a link to share it.

- Speak directly to the person you need to share the information with, preferably by video call or a mobile call that you have initiated to a known number. Use this opportunity to share the information in real-time over video or call so there is no record of it.

- If you must share it via email, test, or messaging app, split the information using different methods and delete those messages after wherever possible.

  Example: Username by email and password or passphrase by text or messaging app.

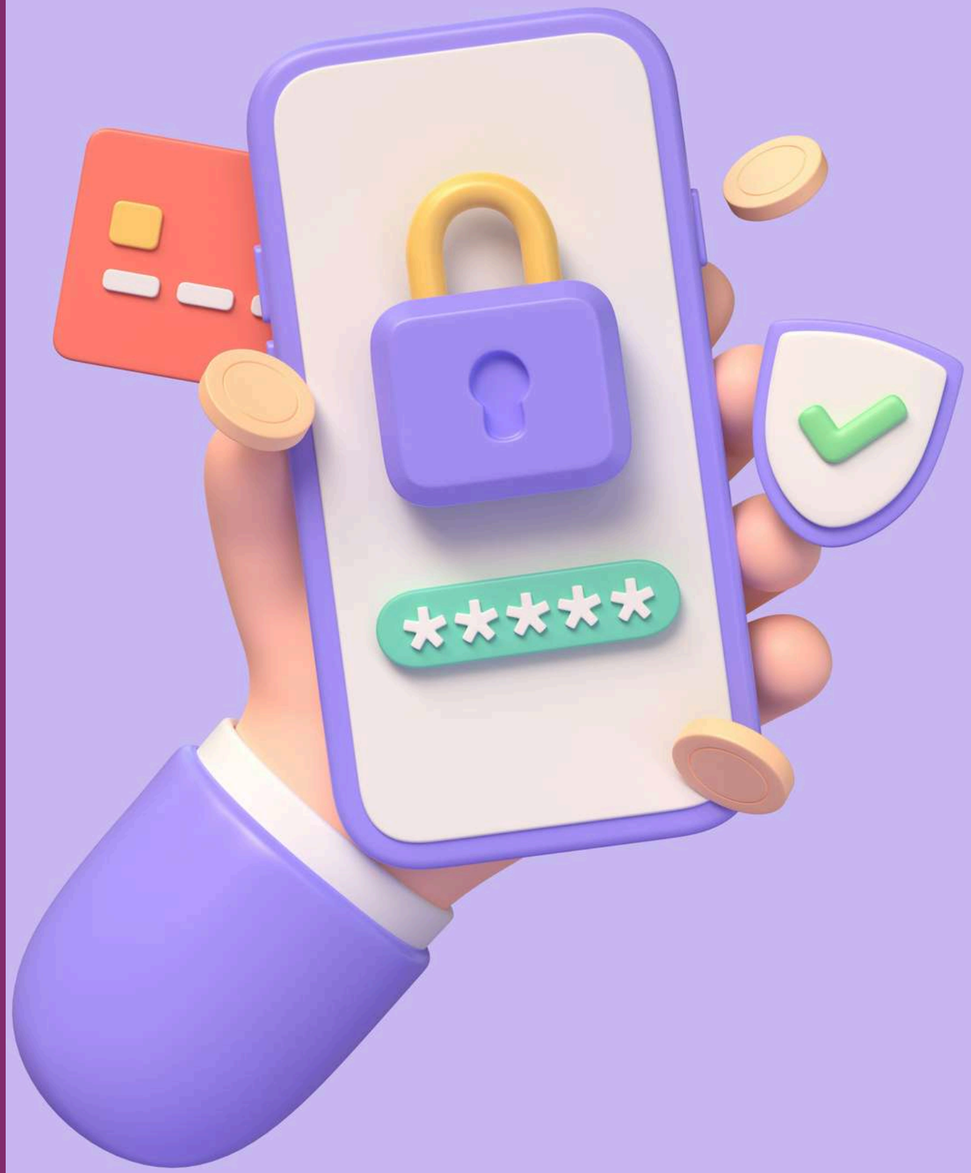
- If you are using two-factor or multi-factor authentication (2FA/MFA) for that account (Congratulations!) then use a third method to give the 2FA code. If you are not using 2FA/MFA yet, please check the later lesson to learn more! Most MSMEs in India will use Gmail for operations. If you're already using 2FA.

Here are some additional layers of security you can introduce into your operations:

- Use an authenticator app like Google Authenticator for generating 2FA codes without requiring SMS.
- Use an alternative email ID registered specifically for recovery, ensuring access even if the primary phone is unavailable.
- Use Indian-specific SMS-enabled banking apps or UPI apps to familiarize employees with secure authentication systems, as they often overlap with personal 2FA experiences.
- If Remind your employees and team members that banks like SBI and ICICI use OTP-based MFA as a standard for their net banking services. This establishes the importance of using multilayered security protocols for all important transactions and processes.

Using a Password Manager

Do you have several or more accounts to manage? Feeling unsure of how you are going to create, save, and remember all of those unique passwords or passphrases we've been discussing? The use of a password manager tool is a great way to navigate all of these challenges. Password managers create and store unique and complex passwords for each of your accounts. Setting up your password manager account will take a small investment of time, but it is well worth it and easy to maintain and update after that initial setup. You will then only need to remember one password (using the skills you already learned on how to create a strong password or passphrase) for the password manager tool itself.



Helpful things to know about password managers:

- You can integrate biometric authentication for an extra layer of security, especially useful for mobile devices in BYOD settings.
- Password managers can help enhance security and manage access for distributed teams with remote workers.
- Strict onboarding and off-boarding protocols must be followed for organisational passwords. Ensure all passwords are changed or removed when employees join or leave.
- While there are several globally-popular tools that can help you with password management, there are some great indigenous options too. Use local solutions (e.g., K7 Password Manager) along with global tools like LastPass or Dashlane.
- MSMEs can prioritise low-cost, India-made solutions when upgrading their security features. The DigiLocker is a key example of Indian security and data management options.Bitwarden is a free, open-source password manager that is secure, ZoHo Password Vault is also recommended.:

Following Safe Password Practices For Online Browsing

Most major Internet browsers also allow you to save your passwords, which is very convenient (and free), however, there are some important things to remember when using them.

Passwords, Password Management, and Two-Factor Authentication

Top tips:

- If you share your device (mobile, tablet, laptop, or desktop) with employees or family members, you are essentially giving them the same access that you have to all of those accounts. This is extremely risky. Don’t save passwords on shared/ public devices

- Ensuring you have two-factor or multi-factor authentication (2FA/MFA) in place for all accounts that allow it is a great layer of additional security to reduce this risk, especially if you choose to require 2FA/MFA for each login. This way, a family member cannot inadvertently access an account without your permission.

- Consider the level of sensitivity of the account you are accessing using this method - is it your banking account? Payroll? Customer data? The more sensitive the data, the more you should be wary of using browser-based password management. A separate tool may be more appropriate for your business.

Passwords, Password Management, and Two-Factor Authentication

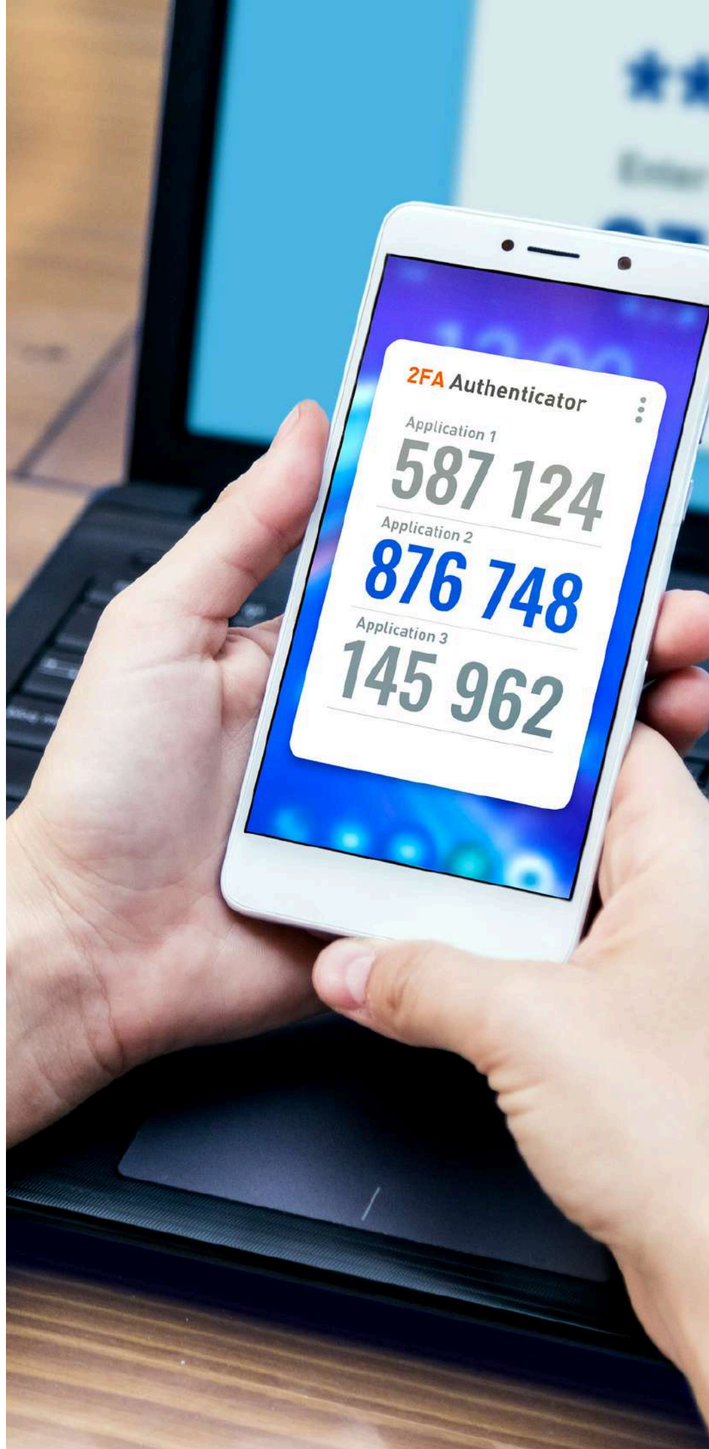
Two-Factor or Multi-Factor Authentication

- Two-factor authentication (2FA), also known as multi-factor authentication (MFA), must be used whenever possible. 2FA requires two separate pieces of information before it gives you access to your account.

  1. Your password or passphrase
  2. Something unique to you. Examples:

- A code that times out using a third-party tool such as Google Authenticator or Microsoft Authenticator
- A code that is sent to your phone or your email
- A biometric, such as a fingerprint or your face

Some accounts only allow one user/admin for the account, so only the main admin can “own” the 2FA code. This creates an extra step in the login process when others have to share those login credentials, however, consider it an additional layer of protection in the event someone gains access to your password or passphrase. Without this code, that person will not be able to gain access to your account. Remember the tips in the lesson talking about sharing login information to accounts and treat it using those same tips.



Passwords, Password Management, and Two-Factor Authentication

A lot of MSMEs in India use Amazon for their e-commerce activities. Since Amazon permits only one admin to set up 2FA, the business owner typically uses their mobile number for the authentication code. Team members needing access must coordinate with the owner to retrieve the 2FA code during login.Treat the 2FA code like an OTP for UPI payments: critical, sensitive, and only to be shared with verified individuals when absolutely necessary.

- Here's a quick list of things to keep in mind regarding 2FA and MFA:

- Enable 2FA for critical accounts (e.g., banking, emails).

- OTPs via SMS or app-based 2FA add a layer of protection.

- Consider MFA options (e.g., biometrics) for added security.

- Be mindful of attempts to extract OTPs and authentication codes - scammers will often call and post as legitimate authorities or service providers and ask for these codes. They might refer to them by other names to confuse you into sharing said digits.

- For accounts that give you a list of recovery codes upfront - store the same in a secure place, ideally not on the device in question.

Strong Passwords Checklist

- **Password Length:** Minimum of 8-12 characters or more.
- **Password Complexity:** Require a combination of uppercase, lowercase, numbers, and special characters.
- **Password Uniqueness:** Enforce unique passwords for each account or system or device. No password reuse.
- **Password Expiration:** Require regular password changes, e.g., every 60-90 days. Prevent reuse of previous passwords.
- **Password Storage:** Store passwords using secure hashing algorithms, never in plain text.
- **Password Management**: Encourage password managers and prohibit password sharing or writing them down insecurely.
- **Password Reset:** Implement secure procedures with multi-factor authentication for password resets.
- **Password Auditing**: Regularly audit password strength and compliance and monitor for compromises.
- **Password Protection:** Use key-based authentication along with passwords where possible.
- **User Awareness:** Provide training on password best practices and risks of weak passwords.
- **Policy Enforcement:** Define mechanisms for enforcing the policy and procedures for granting exceptions.
- **Policy Review:** Regularly review and update the policy to align with best practices and emerging threats
- **Complex Words:** Avoid using passwords that consist of simple dictionary words.
- **Personal Information:** Avoid passwords such as your birthday or your pet's name.
- **Simplistic Passwords:** Don't use common words like "password" or "12345" as these are easily guessed
- **Passphrases:** Use a series of unrelated words (e.g., "sunflower_eagle!forest") for added complexity without compromising memorability.
- **Password Sharing:** Do not share your password unless absolutely necessary.
- **Monitor for Breaches:** Periodically check if your email or password appears in data breaches via services like Have I Been Pwned.

Q&A Session

Any questions or thoughts?

Share with us your queries or thoughts before we proceed to Module 5

APAC Cybersecurity Fund

The Asia Foundation

Thank you for your attention!

For further assistance you can also reach out to the CyberPeace Foundation at 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 Foundation for MSME Clusters (FMC)

with support from Google.org

APAC Cybersecurity Fund

The Asia Foundation

Module 5

Protect Against Phishing and Malware

implemented in India by

with support from Google.org

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 5

What We Will Talk About

Protect Against Phishing and Malware

Phishing tries to trick people into giving up sensitive information or access to money by appearing to be legitimate requests from trusted sources.

Phishing is responsible for 67% of all data breaches, making it one of the most significant attack vectors globally. .

1 CYBER ATTACKS FROM PHISHING

2 HOW ANTI-VIRUS SOFTWARE WORKS

3 RANSOMWARE AND MSMES

4 PHISHING AND MALWARE PROTECTION CHECKLIST

What is Phishing?

Phishing is an email communication with criminal intent. While email is the most common form of phishing,

There are also other methods:

- Phishing = email
- Smishing = SMS/text messages
- Vishing = voice calls or messages
- Quishing = QR codes

We'll discuss each of these in this course but will collectively refer to them as "phishing" throughout the course.

How Do the Criminals Phish?

As a micro or small enterprise, you might not be the target of all of these methods, but you need to be aware of them to protect yourself, especially as your business grows. The more targeted the attack, the more sophistication and research has been conducted by the criminal behind it. Small businesses in India, particularly MSMEs, are targeted disproportionately due to limited cybersecurity resources and high digital adoption.

The use of artificial intelligence only increases the likelihood that the criminals will be successful in their attempts. Attackers now use AI to craft personalized phishing messages that seem authentic. AI-generated deep fakes are also used to impersonate trusted individuals in emails or voice messages. The deep fake video of the late industrialist Ratan Tata asking in 2023, asking viewers to “invest” in a ‘new project’ is a compelling example of how emerging technology is being maliciously used for phishing.

Mass Phishing

- Generally untargeted mass emails sent pretending to be from reputable organizations.
- Often about recent news stories, recent natural disasters, or appear to come from common organizations used by many in the hope that some recipients will respond.
- Often claims of urgency or appealing to your emotions (this is called “social engineering”).
- In 2023, India experienced over 79 million phishing attacks, making it the third most targeted country globally. Attackers used mass phishing campaigns that mimicked popular brands like Microsoft and Amazon to target users in the technology and financial sectors. In the aftermath of the Covid-19 pandemic, mass phishing attacks calling for ‘donations’ and ‘disaster relief’ have also been on a rise.

Spear Phishing

- More targeted emails designed to look like a person or organization that the victim knows or is familiar with (example: from the owner to a new employee who might be eager to please the new boss).
- Because these emails often have a specific objective in mind, usually some research on the intended target is done to improve the chances of a successful attack.
- Example: An “employee email” to the payroll administrator requesting a change of bank account for the employee's paycheck deposits.
- Spear phishing attacks accounted for 64% of targeted email threats globally in recent years, with significant cases reported in India. India’s critical sectors, such as energy and defense, remain frequent targets due to their reliance on email communications.

Whaling Attacks

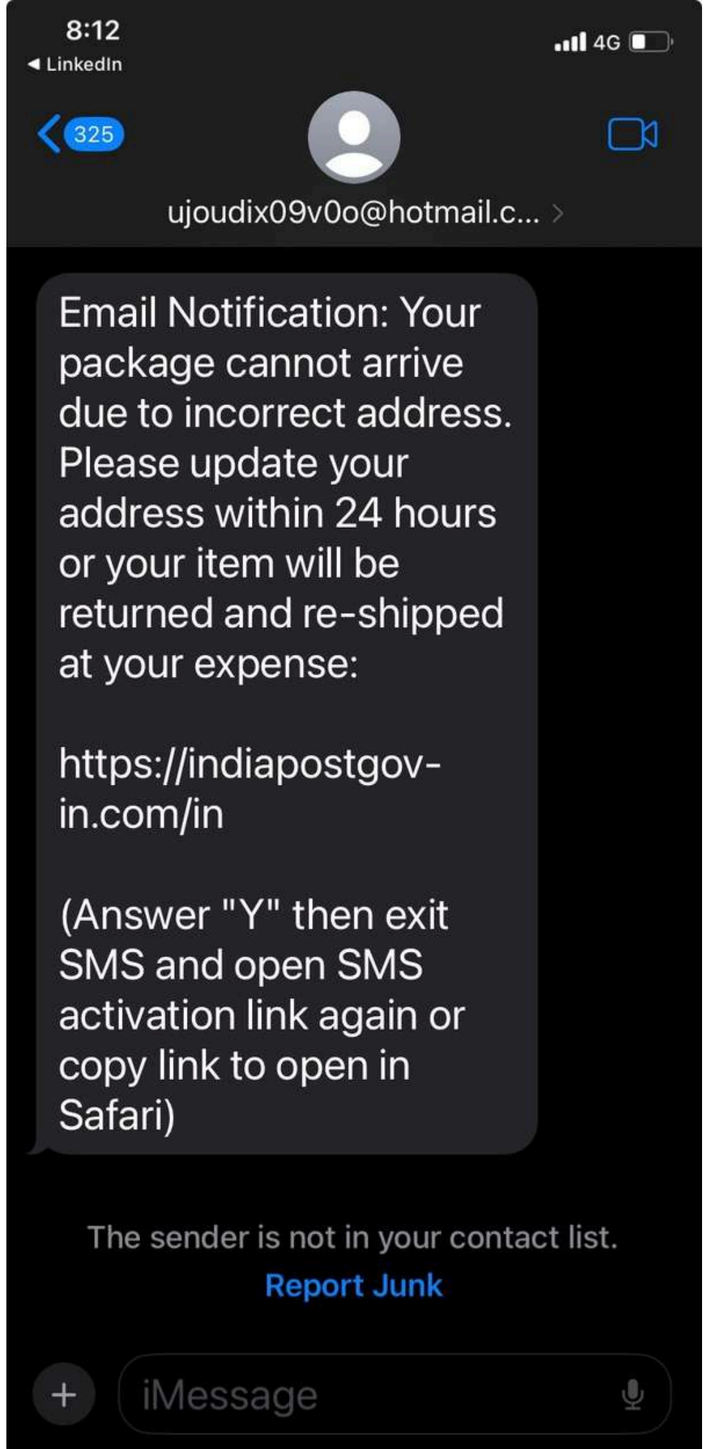
- These are highly targeted attacks, often towards very senior figures within an organization or high-profile individuals.
- Significant research needs to be performed and criminals may have been tracking movements and collecting data for months before making the attack.
- You've likely heard about various business and political leaders whose staff have been duped by these extremely sophisticated whaling attacks.
- The Serum Institute of India was defrauded of Rs 1 crore in a whale phishing attack. The cybercriminals used a phone number with a display picture of the company's CEO, Adar Poonawalla.

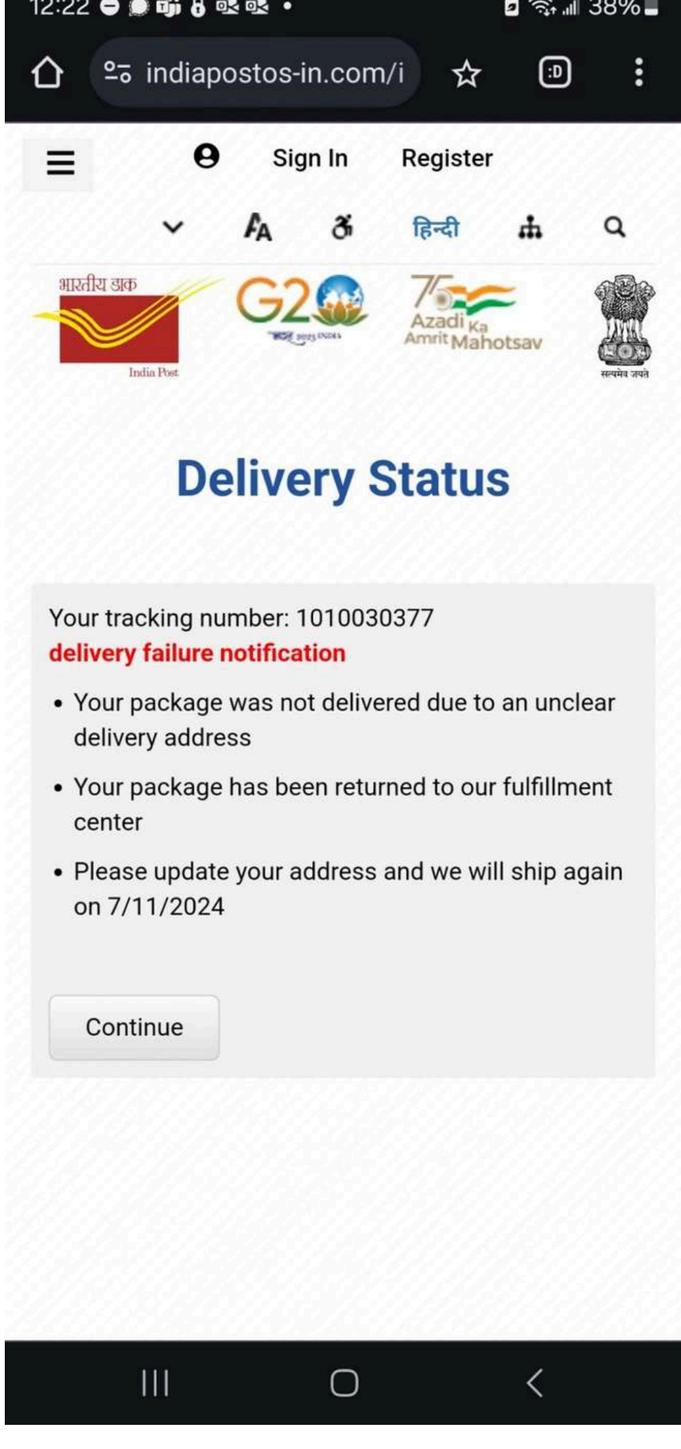
What Does Phishing Look Like?

In the MSME-specific context, deepfakes and false information are used to mislead employees, tricking them into sharing sensitive data and compromising business security/ trade secrets/ proprietary information. Fake customer service messages or HR communications during tax season or festivals are a common luring tactic used against MSMEs in India.

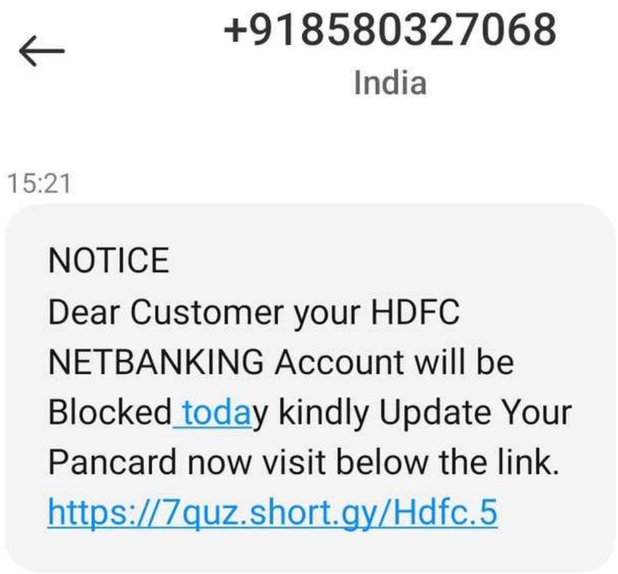
- When the malicious link or attachment is clicked or opened, then the initial attack is successful and the account has been breached.
- Phishing attacks are sometimes used to create a “backdoor”, which is a secret route into your device.
- Criminals can install ransomware that locks you out of your data and demands a ransom be paid in order for you to get it back.

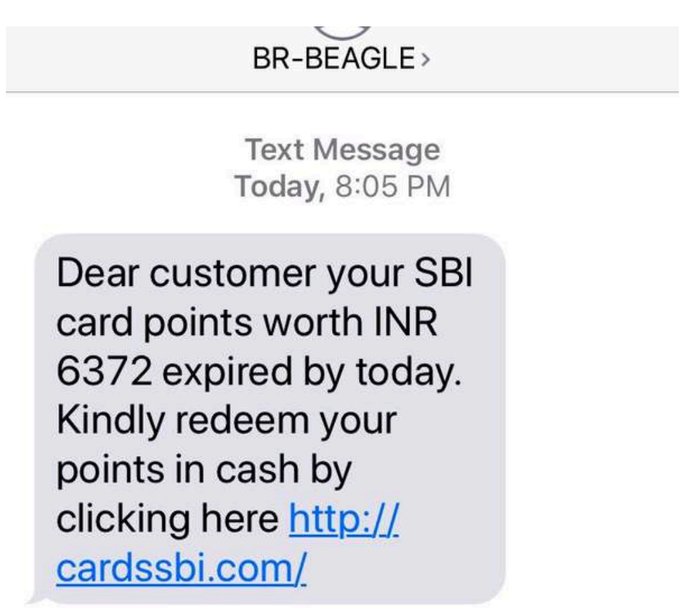
Delivery Phishing Scams in India



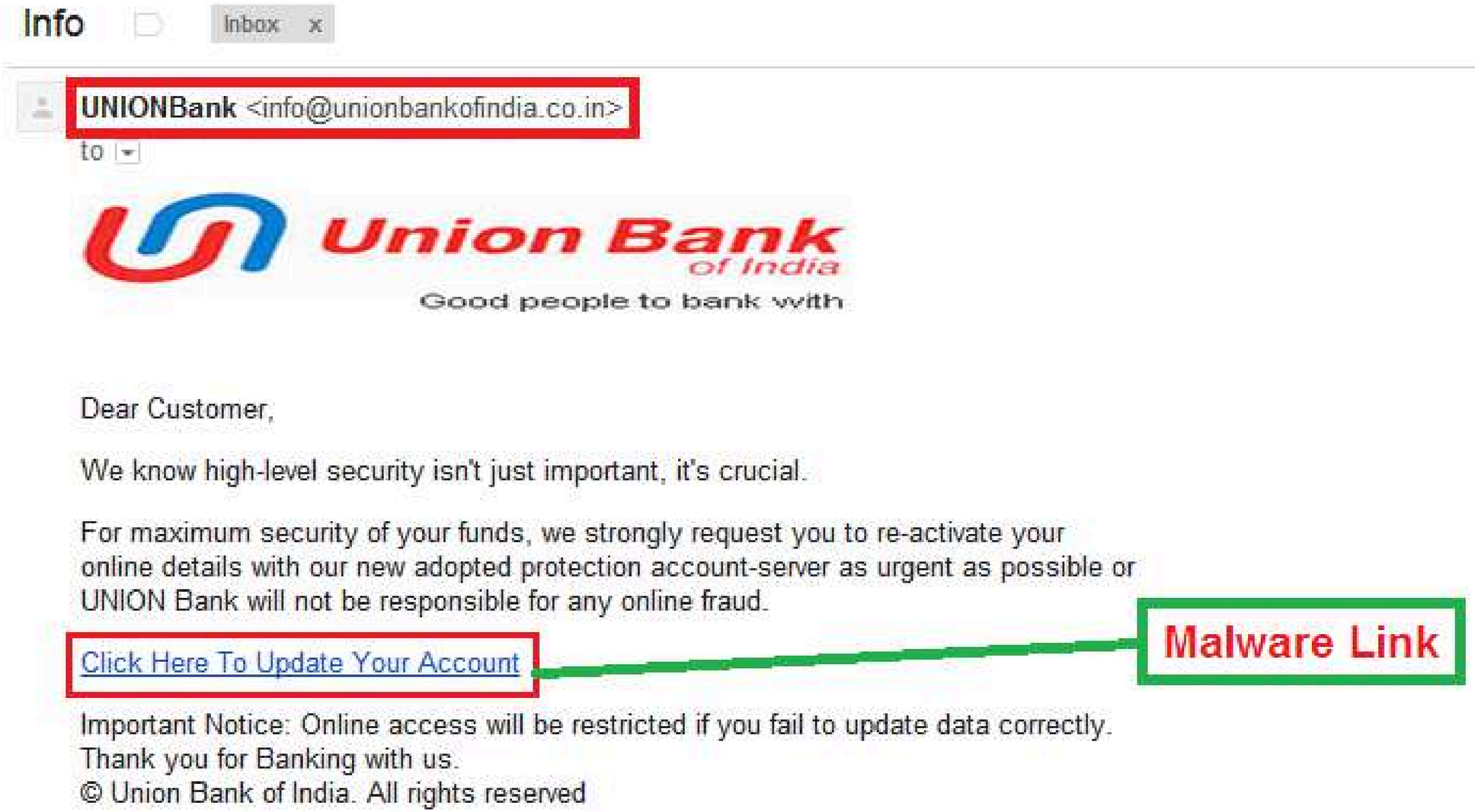


Mobile Banking Phishing Scams in India





Email Phishing Scams in India



The Life Cycle of a Phishing Attempt

- **Planning:** Attackers select targets and craft fake messages
- **Development:** The mode of messaging is worked on. This can be as basic as an SMS and as sophisticated as an A/V AI communication
- **Hook:** Some form of enticement or coercion or compulsion is built into the message
- Execution: Phishing emails or messages are sent to targets
- **Engagement:** Victims unknowingly share information or click malicious links
- **Data Capture:** Victims unknowingly enter sensitive data on fake sites or grant access to their systems
- **Monetization:** Stolen information is used for financial gain or data breaches.
- **Exploitation:** Financial and reputational damage can be accompanied by extortion, blackmail, emotional and mental harassment, intense stress, and social stigma

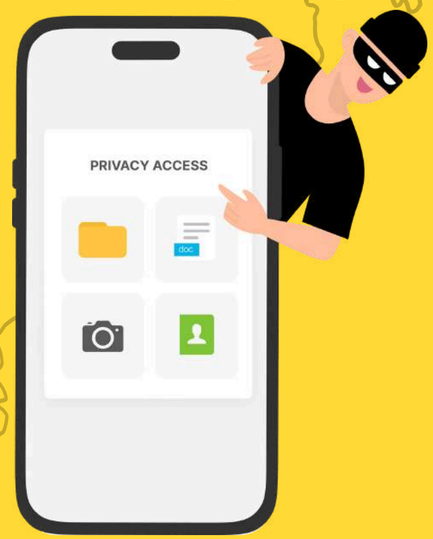
Protect Against Phishing and Malware

Identifying Phishing

Phishing emails are not always easy to spot. Before clicking or opening any email, take a pause and keep these points in mind:

- They may look like they come from someone or some organization you know
- They may have exactly the same email address as someone you know
- They might mimic the logos and format of emails from well-known organizations
- They might refer to recent news events or a job you've just done
- The attacker might have called your company or checked online to personalize the email and to make it look more real add more

Common Phishing Trends in India



- UPI Phishing: Fake UPI payment requests or refund scams.
- Festivals Phishing: Scams around Diwali or holiday discounts, often impersonating e-commerce or banking services.
- QR Phishing: Fake QR codes leading to fraudulent payment pages.
- Language-Specific Phishing: Scams in local languages to increase relatability and trust. Next, we'll look more at exactly what to look for and where.

Protect Against Phishing and Malware

The Warning Signs of Phishing

India is the most targeted country in the Asia-Pacific-Japan (APJ) region for phishing attacks, accounting for 33.12% of all phishing attempts in the region. Microsoft was the most impersonated brand in phishing attempts targeting Indian users, with 43% of attacks mimicking the company. Other commonly imitated platforms include OneDrive, SharePoint, and Adobe, reflecting the widespread use of these services in Indian businesses

Learning To Read Telltale Signs

- Generic Greetings
- Unfamiliar Senders
- Urgent Language
- Misspellings
- Unexpected Attachments
- Request For Sensitive Info
- Typosquatting
- Mismatched URLs

Protect Against Phishing and Malware

How Anti-Virus Software Works

Anti-Virus Quick Facts

- Anti-virus (AV) can help protect you and your system from phishing or other cyberattacks.
- Each virus has specific characteristics, called a signature. Anti-virus (AV) software checks for these signatures, intercepts the virus, disinfects it, and prevents it from reaching the target.
- Attackers create new strains of an existing virus with a slightly different signature. When there isn't a "cure" that exists for this new virus, this is called a "zero day attack."
- Once these new viruses are identified, AV software is quickly updated and devices are protected again. Keep in mind, new viruses are constantly being developed. It is critical to keep your AV software up to date at all times, just like you learned to do with all your software in earlier lessons.

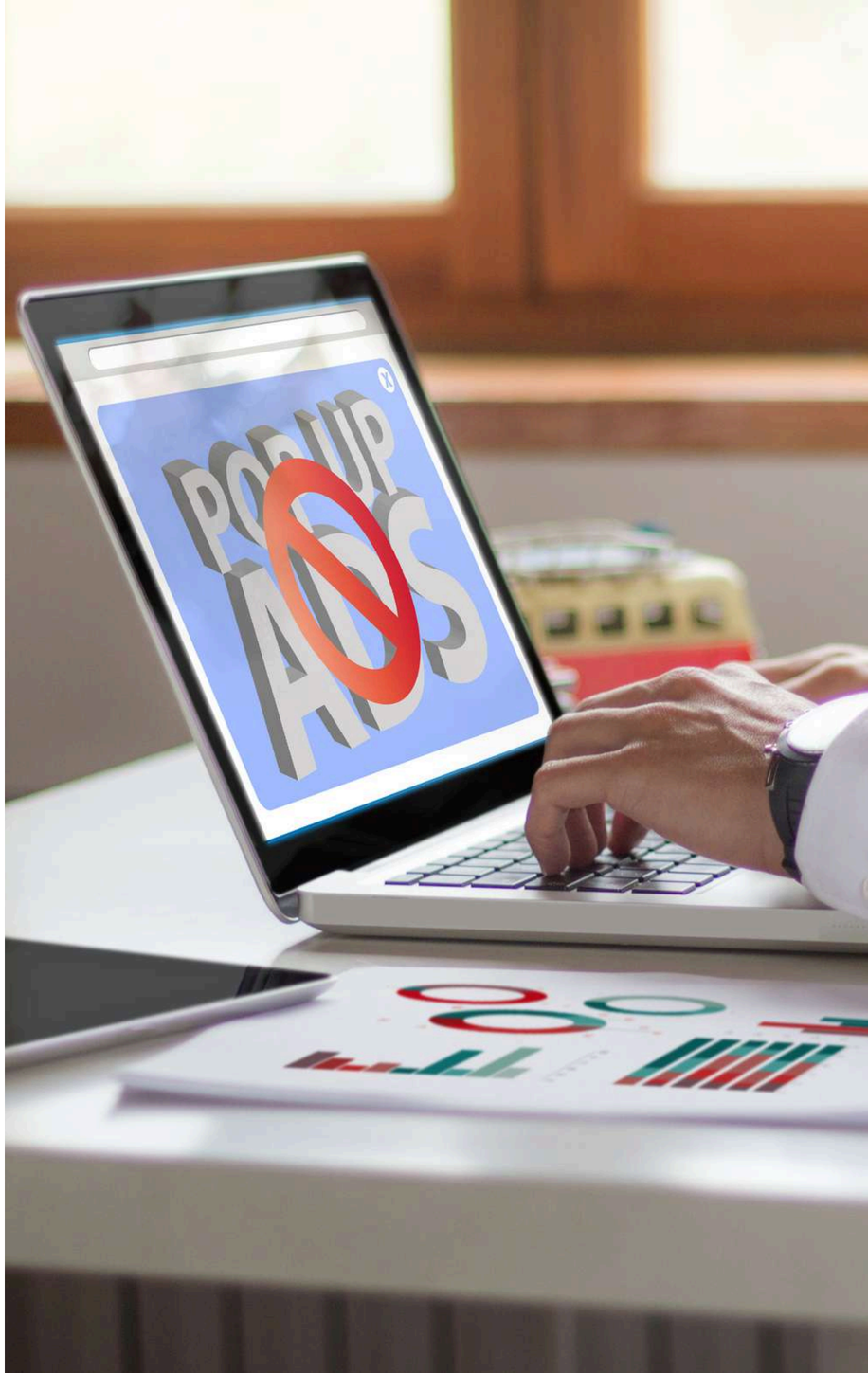
Protect Against Phishing and Malware

Ad Blocking for Browsers

Ad blockers prevent advertisements appearing on web pages while browsing the Internet and deepen your lines of defense against attack.

While many of the website ads or popup messages that appear while browsing are legitimate or useful, many contain malicious code.

Malicious ads accounted for 16% of phishing incidents in India in 2023, primarily targeting mobile users. Pop-up scams often leverage regional language targeting to build trust among first-time digital users. Ad-blockers reduced exposure to such scams by approximately 40%, a statistic that proves just how useful they can be for a small business with a modest budget for cybersecurity



Protect Against Phishing and Malware

Ransomware and MSMEs

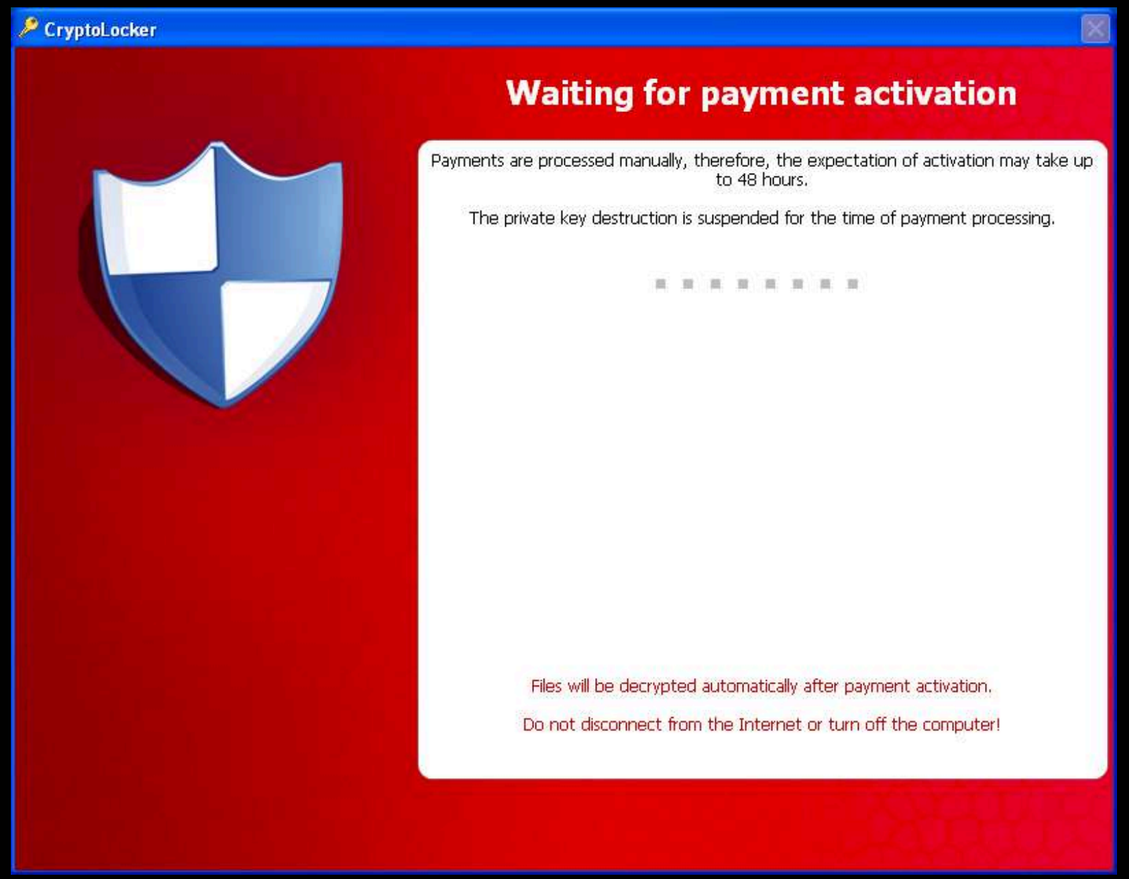
Protect Against Phishing and Malware

What is Ransomware?

Often spread via phishing emails or texts, users unknowingly visit an infected, malicious website, and the criminals gain access to your system and prevent you from accessing your data. They then hold you for ransom for a sum of money before releasing it back to you. Sometimes organizations pay the ransom, only to find that the criminals refuse to release the data.

Ransomware is the single most common cyber threat that MSMEs face. Remember, just because you are small does not mean you are not at risk of falling victim. In 2023, ransomware attacks on Indian SMEs surged by 50%, with average recovery costs of around INR 6-8 lakhs.

Examples of Ransomwares:



Consider the impact, from a financial and reputational perspective, if your business:

- ✓ Was not able to do business for a day?
- ✓ Lost customers because you were unavailable to service their needs?
- ✓ Was no longer able to access customer files or they were corrupted?
- ✓ Was told you could only get access to information if you paid a ransom?

The ransom is usually requested in cryptocurrency (such as bitcoin) which is harder to trace than traditional transfers. Ransomware can be devastating to organizations (large or small).

Anyone with important data stored on their devices is at risk, from MSMEs to large corporations, to government agencies, healthcare systems, and other organizations critical to infrastructure.

The 2022 AIIMS ransomware attack was a high-profile case where attackers encrypted patient data and demanded a ransom of Rs. 200 crore. This incident disrupted healthcare services across India and exposed systemic vulnerabilities. India reported a 120% increase in ransomware attacks from 2021 to 2023. Ransomware accounts for over 21% of cyber incidents in the country, often beginning with phishing emails.

Phishing and Malware Protection Checklist

Keeping Yourself Educated

- Regularly train and update employees on the latest phishing trends.
- Encourage team discussions to share suspicious email experiences as a way to build awareness

Assessing Vulnerability To Phishing

- Run simulations within your organization to test employee responses and identify training needs. These can be digitized or just thought exercises.
- MSMEs should conduct periodic security assessments to identify gaps in their phishing defenses.

Gamified Learning To Protect Against Phishing

- Enjoyable learning
- Increased knowledge
- Skills training
- Higher retention
- Test and measure preparedness against attacks in controlled settings
- Revisit and reinforce concepts through multimedia modules

Q&A Session

Any questions or thoughts?

Share with us your queries or thoughts before we proceed to Module 6

APAC Cybersecurity Fund

The Asia Foundation

Thank you for your attention!

For further assistance you can also reach out to the CyberPeace Foundation at 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 Foundation for MSME Clusters (FMC)

with support from Google.org

APAC Cybersecurity Fund

The Asia Foundation

Module 6

Protecting Your Business and Data with Backups

implemented in India by

Foundation for MSME Clusters (FMC)

with support from Google.org

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 6

What We Will Talk About

Business Continuity and Backups

As more information lives in digital form, backing up your data is critical from a business and personal perspective and crucial for business continuity. This is important no matter what type of device(s) you use: mobile, tablet, laptop, and/or desktop.

Modern reliance on mobile devices and computers means the impact of data loss or downtime can seriously impact or destroy an organization's productivity and profitability. Having backups is absolutely critical to being able to recover quickly and resume business operations after a loss.

Apart from ransomware attacks locking you out of your data, there are many other ways you can lose access to your data. While our focus here is preventing loss or corruption of data due to a cyberattack, backups also help with recovery from hard disc failure, equipment theft, human error, flood or accidental damage, and more.

1. BACKUP BASICS
2. DIFFERENT WAYS TO BACKUP YOUR DATA:
3. CONTINUITY PLANNING
4. DISASTER RECOVERY PLAN FOR YOUR MSME!
5. BACKUP AND RECOVERY CHECKLIST

Backup Basics

Backups are copies of key information or data stored separately from your device. Backups are absolutely critical for every business. If anything happens - cyber-attack, natural disaster, or something else - a backup allows you to quickly restore your data or device and get back to business quicker.

Data backups reduce recovery time, enabling MSMEs to restore operations quickly after disruptions, which is critical for MSMEs reliant on daily cash flow. Legal and financial implications can arise if data breaches, or loss of customer information occur. Backups can mitigate potential legal liabilities by preserving evidence of due diligence.

There are different ways to backup your data:

Offline Backup:

- Offline backup refers to data storage that's both local and offline, such as storage on an external hard drive, USB drive, memory card, or other device.
- These external devices should be disconnected and stored separately from the device itself.
- Store these devices in a safe and secure location. Take into account any environmental factors. For example, if you are in an area with high chances of flooding, store them on the second or third floor.
- Consider affordable external hard drives like Seagate or WD, with encryption features.

There are different ways to backup your data:

Online/Cloud Backups

- Online backups create copies of your important data and store them off-site on secure servers 'in the cloud.'
- Online backups can be set to backup automatically at regular intervals and provide good recovery for many cases (such as theft or flood).
- Take into account the security of the cloud backup. Do they use encryption and two-factor authentication?
- Storing data on cloud platforms like Google Drive, Dropbox, or Microsoft OneDrive is recommended. Local options such as ZNetLive and Netmagic provide secure, cost-effective options for MSMEs.

Continuity Planning

Ensure you have a Disaster Recovery Plan, which helps recovery of critical systems following a disaster (whether accidental, natural, or malicious) and continuity of business operations. Having a plan helps minimize recovery time and damage to systems, helps limit potential liabilities, and can also improve security.

There are many templates and guides for developing a plan available online. Make sure you keep it updated, and conduct mock scenarios to exercise the plan and ensure everyone knows how to implement it. Assign specific employees to monitor and implement continuity plans during incidents.

Let us develop a Disaster Recovery Plan for your MSME!

Step 1: Identify Critical Assets

- Define Key Data and Resources: Make a list of all critical data (e.g., customer information, financial records) and resources (e.g., computers, servers) essential for business operations.
- Prioritize: Rank assets by importance. Focus on assets that would disrupt business significantly if lost.

Tip: For MSMEs, start with essentials like customer data, financial records, and operational processes.

Step 2: Conduct a Risk Assessment

- Identify Threats: List potential risks like cyberattacks, hardware failure, natural disasters, or human error.
- Assess Impact: Estimate the impact and likelihood of each risk on your business operations

Example: If a phishing attack is common in your sector, mark it as a high-priority risk

Let us develop a Disaster Recovery Plan for your MSME!

Step 3: Define Recovery Objectives

- Recovery Time Objective (RTO): Set a target time frame for restoring operations (e.g., within 24 hours of an incident).
- Recovery Point Objective (RPO): Determine the acceptable amount of data loss, typically measured in time (e.g., a few hours of data)

Step 4: Outline Backup Strategies

- Choose Backup Types: Select offline (external hard drives) and online (cloud) backup methods based on your RPO.
- Schedule Regular Backups: Set automatic daily or weekly backups for essential data.

Tip: For low-cost options, consider rotating external storage devices weekly.

Step 5: Develop an Incident Response Process

- Assign Roles: Identify key personnel responsible for specific tasks in a disaster recovery scenario.
- Create a Response Flowchart: Outline steps to take immediately after an incident, including reporting protocols, backup checks, and restoration processes.

Step 6: Create a Communication Plan

- Internal Communications: Decide how to inform employees during an incident and assign spokespersons for updates.
- External Communications: Plan how to notify clients, suppliers, and stakeholders if their data or services are affected.

Tip: Have templates ready for emails and messages to reduce response time.

Step 7: Document and Test the Plan

- Document Procedures: Write down each step, including details on accessing backups, contacting support, and restoring data.
- Run Simulations: Conduct drills quarterly to ensure staff are familiar with the plan and backup processes work smoothly.
- Update Regularly: Review and update the plan as your business evolves or as new risks emerge

Backup and Recovery Checklist

Backup & Recovery Essentials

- Schedule automatic backups for high-priority data.
- Store backups in multiple locations (offline and cloud).
- Set up alerts to notify when backups are complete or fail.

Sector-specific Recovery Priorities Retail MSMEs

- Customer data, sales records, and inventory.
- Manufacturing MSMEs: Production data, supplier contacts, machinery configurations.
- Service MSMEs: Client data, project records, invoicing details.

Protecting Your Business and Data with Backups

Backup and Recovery Checklist

Risk & Priority Mapping

- Identify all important data assets within the MSME, including customer information, financial records, intellectual property, and operational data
- Check for all probable attack sources, including phishing, malware, ransomware, data breaches, and accidental deletion.
- Check existing security measures and identify weaknesses like outdated OS, employee training, periodic security checks
- Calculate the impact of vulnerability exploits for each asset, using either a simple qualitative scale or a more quantitative approach.
- Create a prioritized list of risks based on their potential impact and likelihood.
- Develop Mitigation Strategies which may include updating security software, limiting access, improving physical security, and an established backup and recovery procedure

Backup and Recovery Checklist

Map Data Based On Risk Categories

- Financial DataBank details, tax documents.
- Customer Data: Personal information, order history.
- Operational Protocols: Employee records, product details.

Google Drive

Low-cost Hardware & Other MSME-Friendly Solutions

- Basic external hard drives
- USB sticks for physical backups
- Budget-friendly cloud plans like G-Drive for online storage

Q&A Session

Any questions or thoughts?

Share with us your queries or thoughts

APAC Cybersecurity Fund

The Asia Foundation

Thank you for your attention!

For further assistance you can also reach out to the CyberPeace Foundation at 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 Foundation for MSME Clusters (FMC)

with support from Google.org