APAC Cybersecurity Fund

The Asia Foundation

Module 5

Protect Against Phishing and Malware

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 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

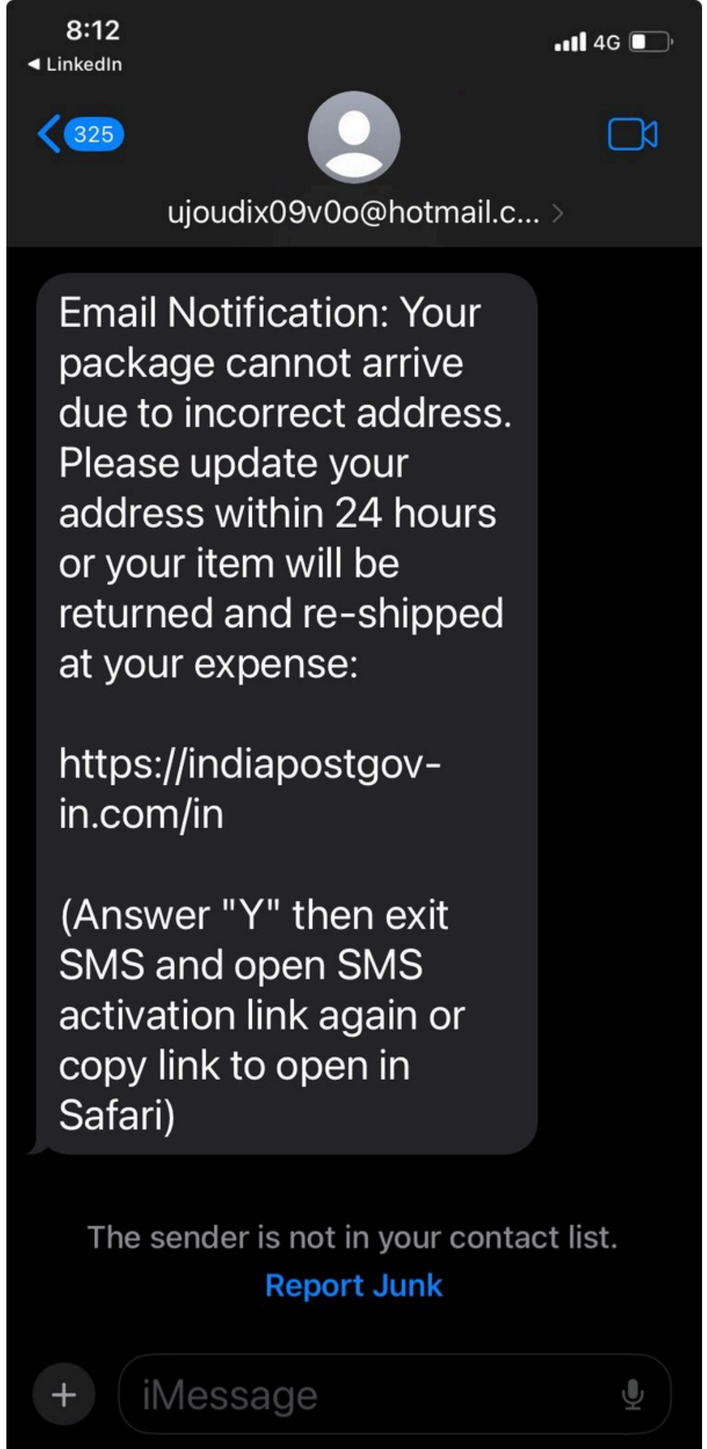
- These are highly targeted attacks, often towards very senior figures within an organization or high-profile individuals.
- Significant research needs to be performed and criminals may have been tracking movements and collecting data for months before making the attack.
- You've likely heard about various 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.

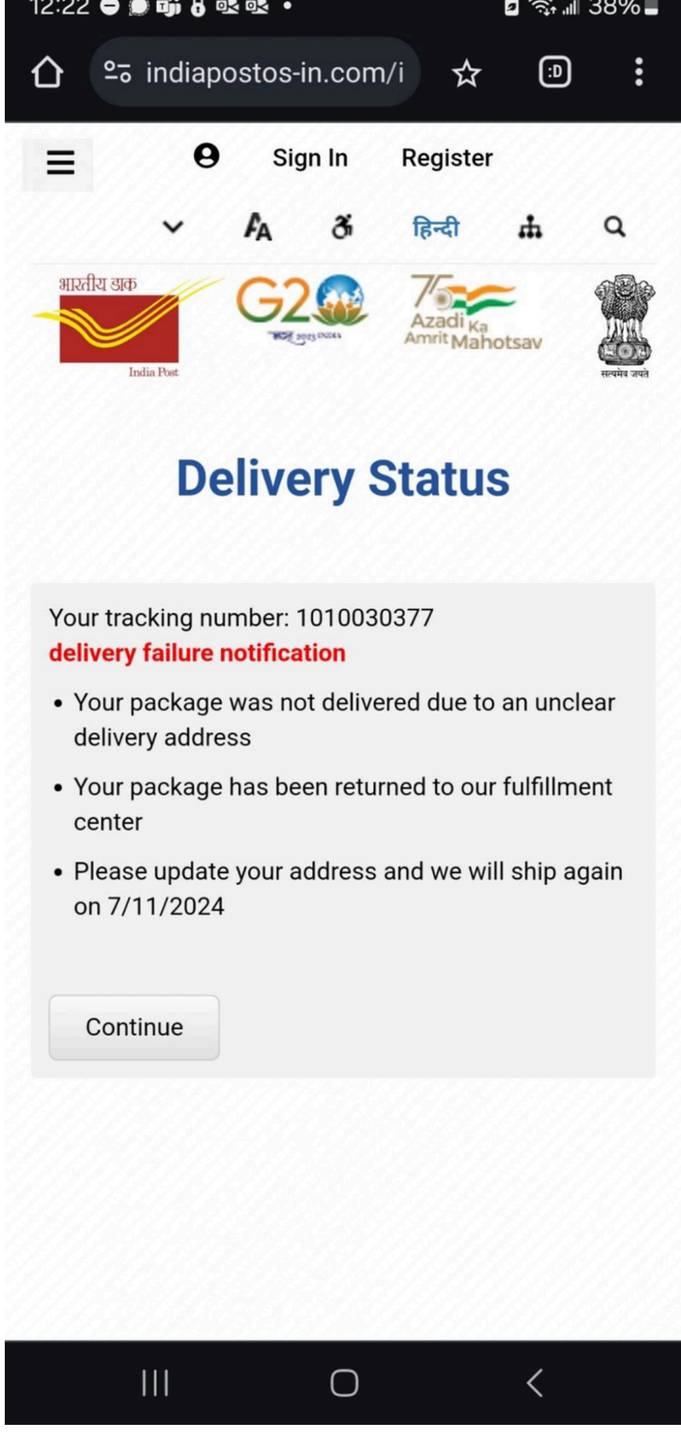
What Does Phishing Look Like?

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.

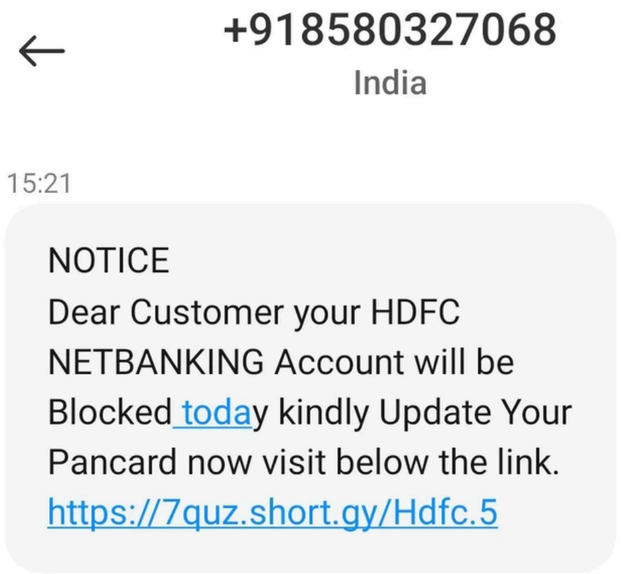
- When the malicious link or attachment is clicked or opened, then the initial attack is successful and the account has been breached.
- Phishing attacks are sometimes used to create a “backdoor”, which is a secret route into your device.
- Criminals can install ransomware that locks you out of your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

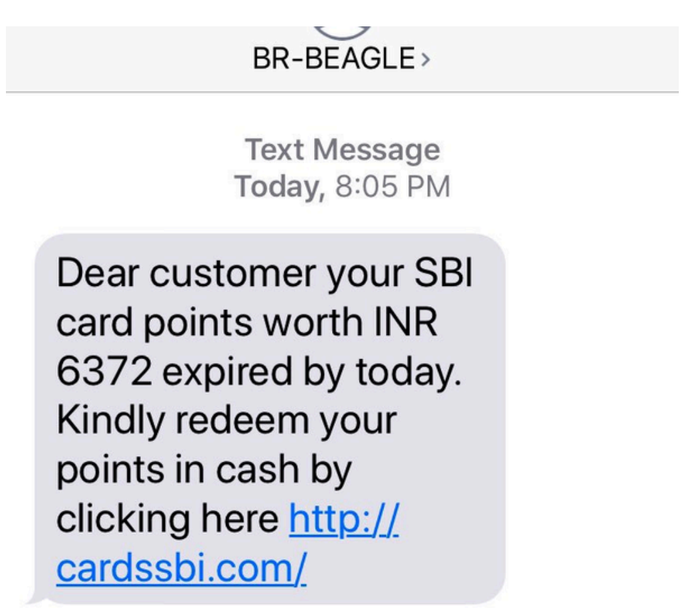
Delivery Phishing Scams in India

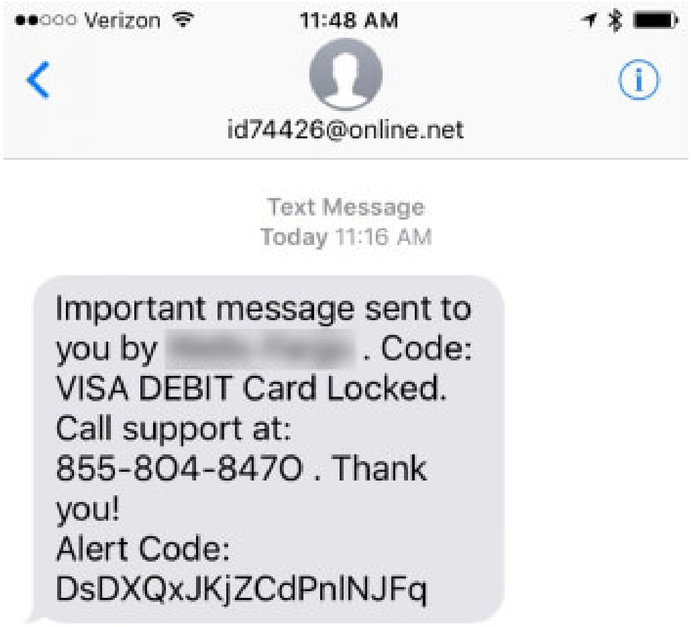




Mobile Banking Phishing Scams in India







Email Phishing Scams in India

Info Inbox x

UNIONBank <info@unionbankofindia.co.in>
to

Dear Customer,

We know high-level security isn't just important, it's crucial.

For maximum security of your funds, we strongly request you to re-activate your online details with our new adopted protection account-server as urgent as possible or UNION Bank will not be responsible for any online fraud.

Click Here To Update Your Account

Malware Link

Important Notice: Online access will be restricted if you fail to update data correctly.
Thank you for Banking with us.

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

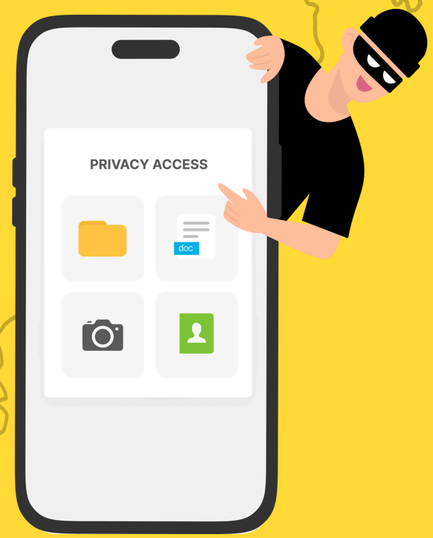
Protect Against Phishing and Malware

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.

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.

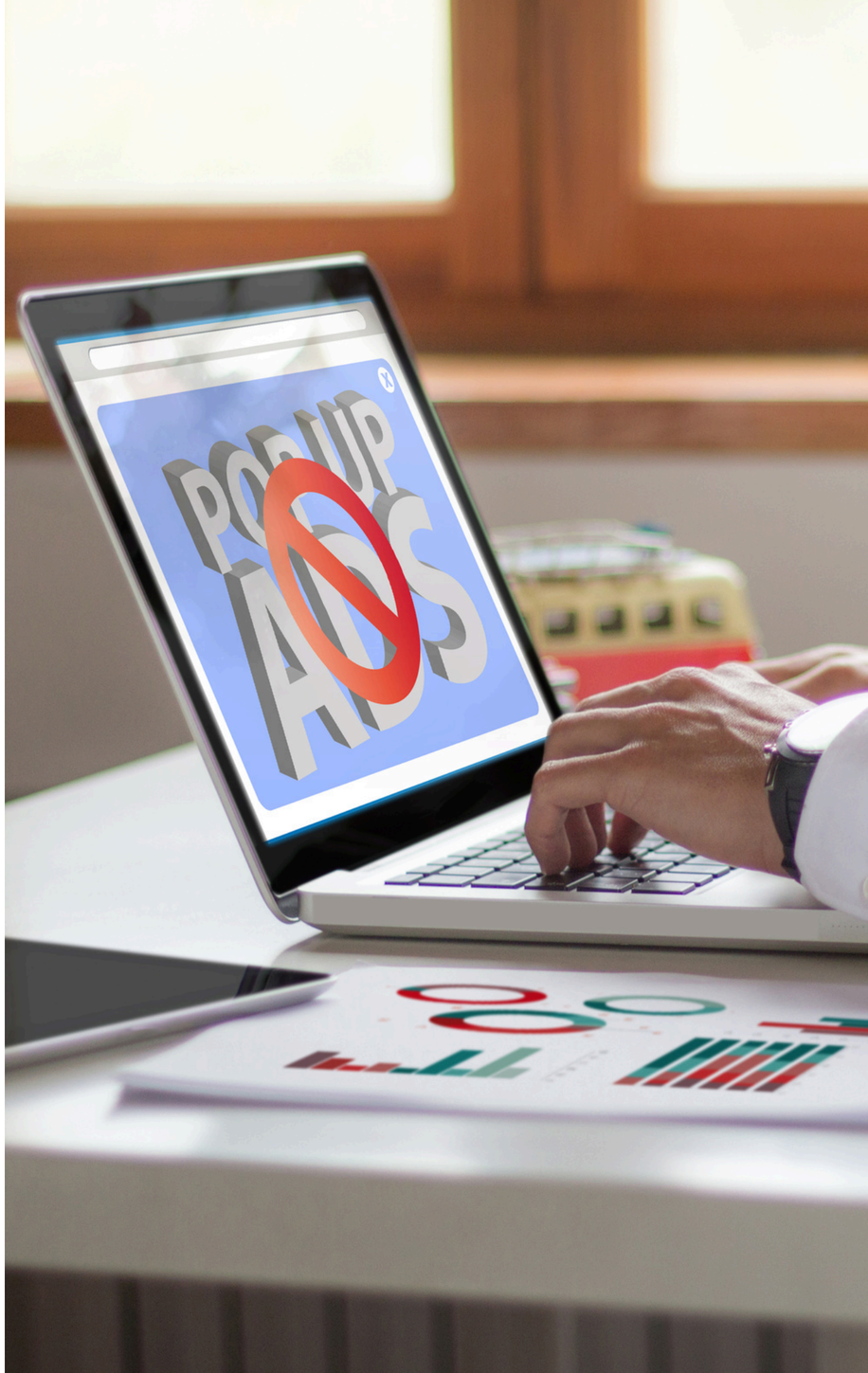
Protect Against Phishing and Malware

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

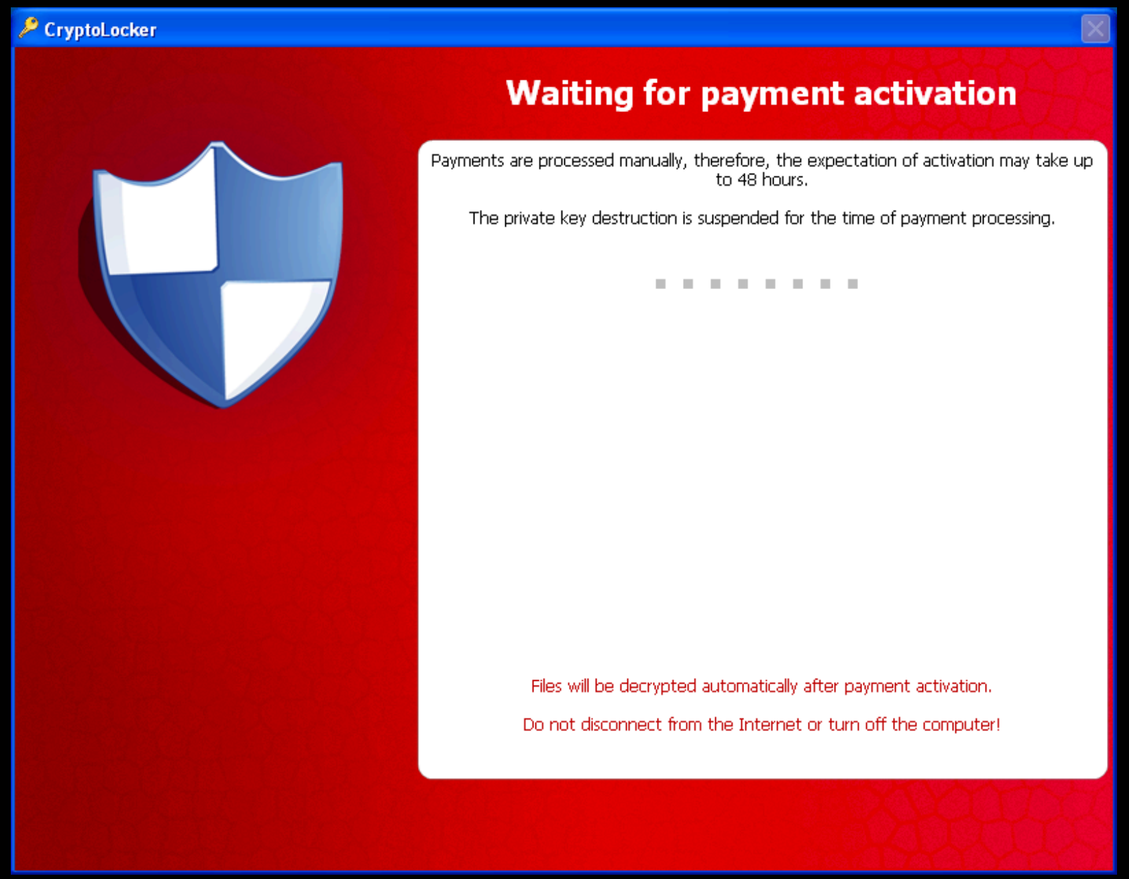
Protect Against Phishing and Malware

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