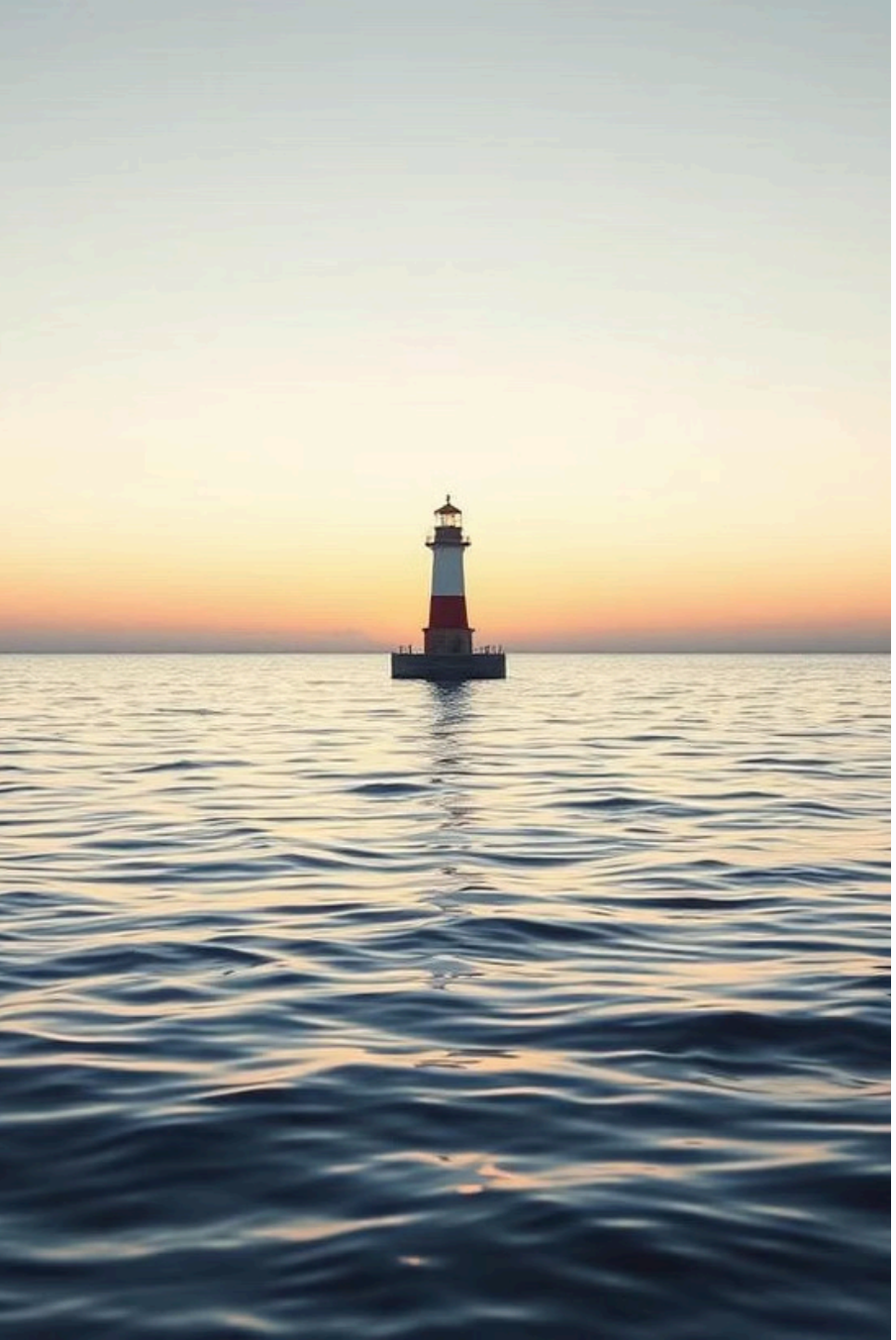


Navigating the Digital Seas: A Guide to Phishing Awareness

Empowering you to recognise, resist, and report phishing attempts.

Made with GAMMA

Understanding the Phishing Menace: What It Is and Why It Matters

What is Phishing?

Phishing is a cybercrime where attackers impersonate trustworthy entities to trick individuals into revealing sensitive information, like passwords or financial details.

How it Works

Typically, it involves deceptive emails, messages, or websites designed to look legitimate, coercing victims into clicking malicious links or downloading infected attachments.

Why it Matters

Phishing can lead to identity theft, financial fraud, and data breaches, severely impacting individuals and organisations alike. It's a pervasive threat in today's digital landscape.

Made with GAMMA

Unmasking Phishing Attacks: Common Scams to Watch Out For

Email Phishing

Deceptive emails pretending to be from banks, government agencies, or well-known companies, asking for urgent action or personal information.

Smishing (SMS Phishing)

Malicious text messages with links to fake websites or requests for sensitive data, often disguised as delivery notifications or bank alerts.

Vishing (Voice Phishing)

Fraudulent phone calls impersonating legitimate entities, pressuring victims to disclose personal details or perform financial transactions.

Spear Phishing

Highly targeted attacks customised for specific individuals or organisations, often leveraging personal information to appear more credible.

Made with GAMMA

Spotting the Imposters: How to Identify Phishing Red Flags

Suspicious Sender

Check the sender's email address for inconsistencies or unusual domains.

Generic Greetings

Be wary of emails that use generic salutations instead of your name.

Urgent Language

Threatening or overly urgent language designed to create panic and prompt immediate action.

Grammar & Spelling Errors

Numerous grammatical mistakes or typos are often indicators of a phishing attempt.

Malformed Links

Hover over links to see the actual URL. If it doesn't match the sender, don't click.

Unusual Requests

Requests for personal or financial information that legitimate organisations would not ask for via email or SMS.

Made with GAMMA

Fortifying Your Defences: Technical Safeguards Against Phishing

Enable Multi-Factor Authentication (MFA)

MFA adds an extra layer of security, making it harder for attackers to access accounts even if they have your password.

Use Antivirus and Anti-Malware Software

Keep your security software updated to detect and block malicious websites and files.

Keep Software Updated

Regularly update your operating system, web browsers, and applications to patch security vulnerabilities.

Implement Email Filters

Utilise spam filters and email security solutions to block suspicious emails before they reach your inbox.

Made with GAMMA

Your Personal Shield: Best Practices to Avoid Phishing Scams

Think Before You Click

Always pause and scrutinise emails or messages before clicking on links or opening attachments.

Verify the Sender

If suspicious, contact the organisation directly using official contact information, not the details provided in the email.

Use Strong, Unique Passwords

Create complex passwords for different accounts and consider using a password manager.

Be Sceptical of Urgent Requests

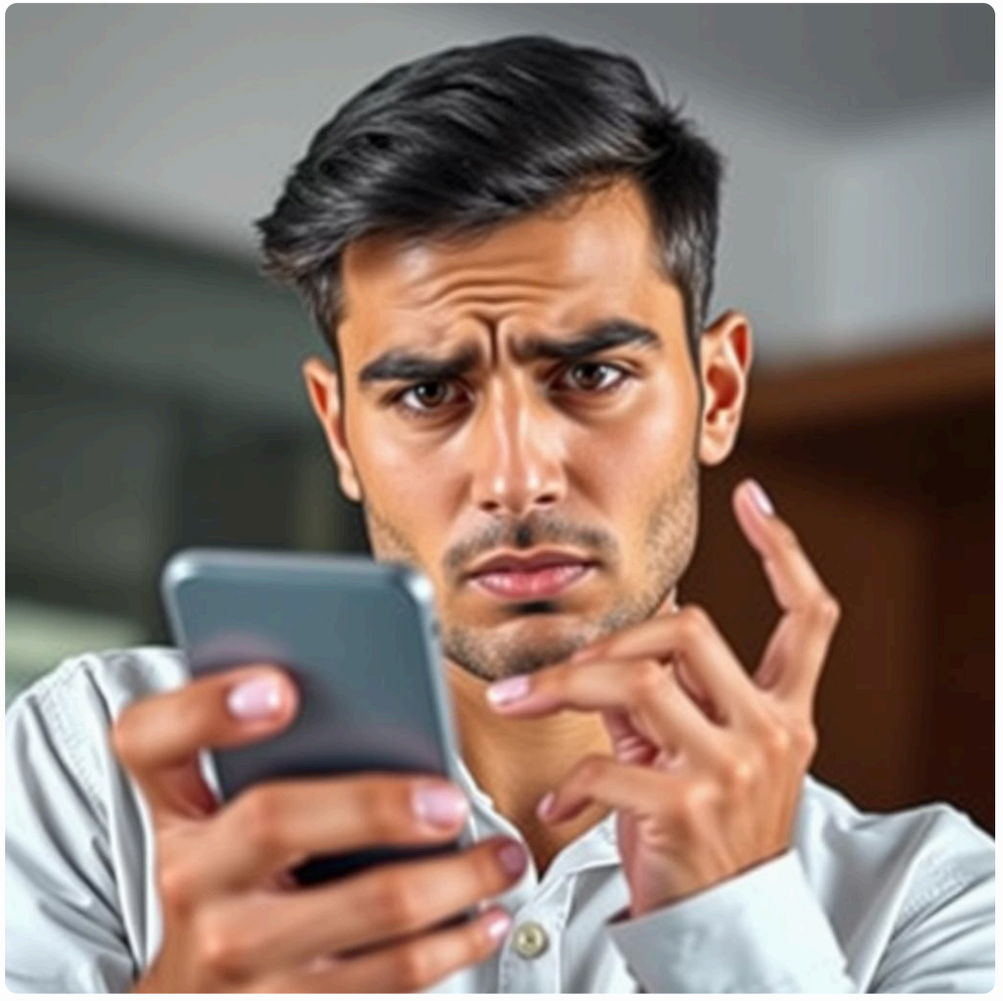
Legitimate organisations rarely demand immediate action or personal information via unsolicited messages.

Report Phishing Attempts

Forward suspicious emails to official channels like the Indian Cybercrime Coordination Centre (I4C) or your IT department.

Made with GAMMA

Real-World Scenarios: Learning from Recent Phishing Incidents in India



Bank KYC Update Scams

Many individuals in India have fallen victim to SMS phishing scams disguised as bank KYC (Know Your Customer) updates, leading to unauthorised transactions.

Electricity Bill Fraud

Scammers send fake electricity bill messages, threatening disconnection unless immediate payment is made via a fraudulent link, resulting in financial loss.

Job Offer Scams

Phishing attempts posing as lucrative job offers, often asking for registration fees or personal details, targeting job seekers.

COVID-19 Related Frauds

During the pandemic, numerous phishing campaigns exploited public fears, offering fake vaccines or relief funds to steal information.

Made with GAMMA

Stay Cyber-Safe: Key Takeaways and Next Steps for You

Stay Vigilant

Phishing attacks are constantly evolving; staying informed is your best defence.

Practice Good Cyber Hygiene

Regularly update software, use strong passwords, and enable MFA on all accounts.

Report and Share Knowledge

If you encounter a phishing attempt, report it and educate others to prevent further incidents.

Continuous Learning

Stay updated on the latest phishing tactics and cybersecurity best practices.

Together, we can build a safer digital environment.

Made with GAMMA