Why Cybersecurity Matters

Protect data	Prevent theft of personal & organizational information.
Prevent financial loss	Stop phishing, ransomware, fraud
Safeguard sensitive documents	Maintain confidentiality & integrity.
Protect reputation	Breaches damage trust in individuals & organizations.
Maintain continuity	Attacks like ransomware disrupt operations.
Public trust	Strong security sustains confidence in digital services.

Employee Responsibilitie

- Recognize threats: phishing, malware, social engineering.
- Use strong, unique passwords + MFA.
- Follow safe web/email habits.
- Handle sensitive data carefully.
- Avoid unapproved apps/devices for work.
- Stay vigilant: lock screens, avoid suspicious links, report issues.
- Share best practices, report incidents promptly.

Red Flags checklist

Sender Email Address	Look for misspellings, slight changes, or unknown senders.
Urgent or Fearful Language	Beware of urgent phrases like “immediate action” or “account suspended.”
Suspicious Links & Attachments	Hover over links and check file extensions to spot threats.
Poor Grammar & Spelling	Typos and errors can signal phishing; legit firms are proofread.
Requests for Personal/Financial Info	Beware of unexpected emails requesting sensitive info.
Unusual Content	Watch for generic greetings, odd content, or unusual tone.

How to Respond

Ask Yourself

> Do I know the sender? Was I expecting this? Does the language/tone match what I know of them? 1. Does the email/domain look correct?

How to Respond (cont)

Never

> Click suspicious links. Download unexpected attachments. Send sensitive info by email. Reply to attacker.

Always

> Verify via phone/in-person/official channel. Report to cybersecurity team.

Types of phising

Email	Create urgency to trick victims into giving information, logging in, or sending money.
Vishing (via phone)	Phone scam where attackers impersonate trusted entities to steal information.
Smishing (via text)	Text scam impersonating a trusted entity to steal data or money.
Emerging Methods	- Deepfake voice/video impersonation. - Business Email Compromise (BEC 2.0). - QR Code phishing (“Quishing”). - Collaboration tool phishing (Slack/Teams/Zoom). - Consent phishing (malicious OAuth permissions). - Search engine phishing (fake ads & portals). - Calendar invite phishing.

Elements of Phishing attacks

Impersonation	Appears legit with official logos, formatting, and language.
Persuasive Language	Uses emotions, threats, or rewards to prompt action.
Sense of Urgency	Pressures victims with urgent security threats or account issues.
Malicious Links	Sends victims to fake sites or numbers to steal data.
Dangerous Attachments	May hide malware in fake invoices or receipts.
QR code	Qr code to login pages or asking for concent of OAuth
Invites	Fake calender invites or shared docs
Voice Messages	These are usually AI generated

Sponsored by **Readable.com**
Measure your website readability!
https://readable.com

Spam Emails

Spam emails steal data, harvest addresses, or spread malware.

Examples

1. Promotions (fake discounts, giveaways)
2. Job Scams (fraudulent employment offers)
3. Lottery Scams (fake winnings, prize claims)
4.Phishing Attempts (deceptive messages to steal information)

Key Characteristics

I. Unsolicited & unwanted (a.k.a. junk email)
II.Mass-distributed to many recipients
III.Can be part of phishing campaigns
IV.Often linked to advertising or fraud

Spoofing

Forged “From” field to look like a trusted sender.

Used to power phishing/social engineering.

Examples : Fake PayPal or Microsoft addresses.

Sponsored by **Readable.com**
Measure your website readability!
https://readable.com