EMPOWER YOUR EMPLOYEES

The Do's & Don'ts of Phishing

DO:

- **Hover over links to see the true destination**

  Phishing emails often disguise malicious URLs behind seemingly legitimate text. Hovering over the link reveals the actual address before clicking.

- **Verify information independently**

  If an email claims to be from a specific company or organization, contact them directly through their official website or phone number to confirm the message's legitimacy.

- **Look for security indicators**

  Legitimate companies often display security certifications or trust seals on their emails. Their websites also typically use HTTPS encryption, indicated by a padlock symbol in the address bar.

- **Use strong passwords and enable two-factor authentication**

  This adds an extra layer of security to your online accounts, making it harder for attackers to gain access even if they obtain your password.

- **Stay informed about current phishing tactics**

  Regularly discuss new phishing scams and techniques with your team to keep their awareness sharp.

DON'T:

- **Download files from unknown sources**

  Only download files from trusted sources and be cautious of unsolicited attachments, even if they appear harmless.

- **Respond to emails demanding immediate action**

  Phishing emails often pressure you to act quickly without thinking. Take your time to verify the sender and the message's legitimacy before responding.

- **Share personal information through email or text message**

  Never share sensitive information like passwords, credit card numbers, or Social Security numbers through email or text message, even if the sender appears legitimate.

- **Panic or feel pressured**

  Phishing emails often rely on fear and urgency to manipulate you. Stay calm and remember that legitimate companies rarely use such tactics.

- **Ignore suspicious activity**

  If something feels off, even if it's a seemingly minor detail, report it to your IT department. It's always better to be safe than sorry.