Familiarize yourself with phishing attacks

HR & Marketing

What is phishing?

- Phishing is a social engineering act where the perpetrator or attacker attempts to deceive individuals into providing sensitive information.
- This information may include usernames, passwords, credit card numbers, and other Personal Identifiable Information (PII)
- The attacker masquerades as a trustworthy entity or insider in emails, websites, and even text messages.

Key features of phishing

- **Impersonation:**
  Attackers often pretend to be reputable companies, financial institutions, or even trusted contacts

- **Urgency:**
  The body of the message (and sometimes, the email title) often creates a sense of urgency, claiming that an account will be closed or suspended unless a specific action is taken (e.g., clicking a link and adding personal details)

- **Links to fraudulent websites:**
  These emails contain links (sometimes masked in action texts) to harmful or fraudulent websites designed to look legitimate. The sites often capture login credentials.

- **Request for Personal information:**
  Victims are asked to enter PII or other sensitive information that can be used for fraudulent activities.

Learn to spot phishing emails

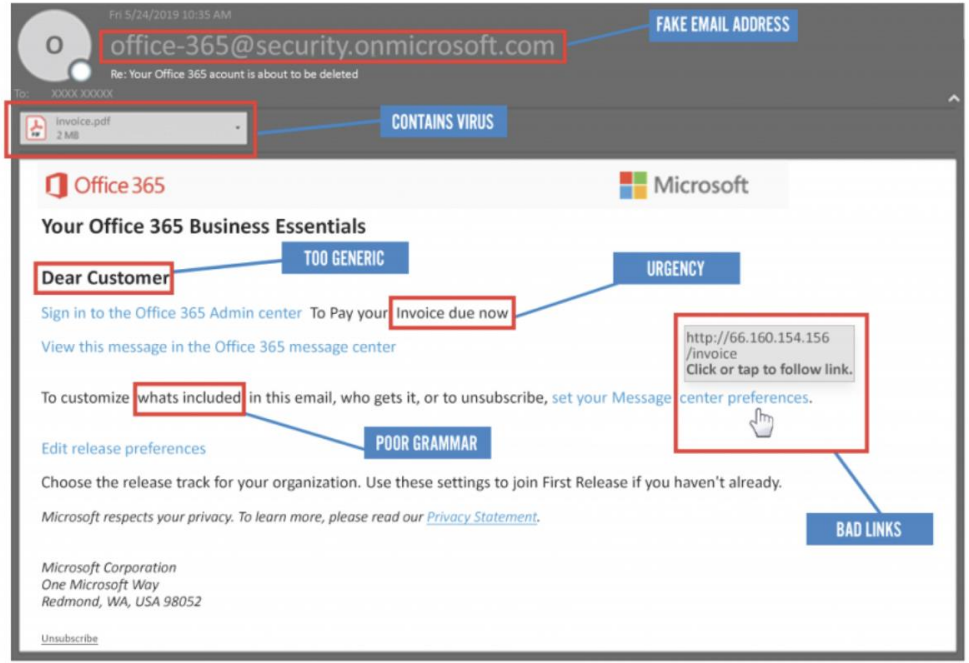

Image: How to spot phishing emails
URL: [7 Ways to Detect a Phishing Email (linkedin.com)]

How do we stop getting phished?

- Do due diligence on the email sender and the message from unsolicited email addresses
- Always hover over links to see the actual URL before clicking to ensure it matches a legitimate search
- Be skeptical
- Report any suspicious email to IT and Management
- Regularly take updated training on phishing and other cybersecurity threats on the company's intranet.

Remember

- Check the URL of the website.
- Always be suspicious of any email requesting personal information.
- Use a password manager to securely store unique passwords for each website.
- Use a secondary/side channel to double-check when someone requests you to do something