Who does the problem affect?

Real-life phishing stories demonstrate how any company or individual may become a target and, sadly, a victim. Phishers aren't too specific about who they want to draw in with their schemes—they often cast as wide a net as possible, dragging in numerous people regardless of their job title, skill, or industry.

Targets aren't just the upper management of a company; the truth is, anybody can be a victim. Even random targeting can allow phishers to gather sensitive information about anyone online, such as their contact details and financial data, which they will use to their advantage.

What is the issue?

Phishing is a type of social engineering attack often used to steal user data, including login credentials and credit card numbers. It occurs when an attacker, masquerading as a trusted entity, dupes a victim into opening an email, instant message, or text message. The recipient is then tricked into clicking a malicious link, which can lead to the installation of malware, the freezing of the system as part of a ransomware attack or the revealing of sensitive information. An attack can have devastating results. For individuals, this includes unauthorized purchases, the stealing of funds, or identify theft.
Moreover, phishing is often used to gain a foothold in corporate or governmental networks as a part of a larger attack .

What is the Impact of the Issue?

The major effects of web phishing are identity theft and monetary loss. Identity theft is a major fear for most consumers as a result of the awareness created by the media.
Monetary loss impacts both consumers and the corporate brands. For consumers, phishing usually translates to direct monetary loss via theft. For the label, it leads to rising costs of prevention and remediation, and soft monetary loss as a result of brand erosion and undermined consumer trust.

What would happen if we didn't solve the problem?

If we don't stop web phishing,then there may be

- Reputational damage
- Loss of custom
- Loss of company value
  Breaches don't just affect consumer confidence. They impact investor confidence, too.
- Business disruption
  No matter how small they might be, breaches inevitably lead to business disruption.

Phishing attacks can paralyse a business. Staff might be unable to continue their work. Data and assets might be stolen or damaged. Customers might be unable to access online services. Most businesses are able to restore operations within 24 hours. But in cases with a material outcome – including a loss of money or data – 41% of businesses take a day or more to recover.

How to safeguard against web phishing ?

- Deploy a SPAM filter that detects viruses, blank senders, etc.
- Keep all systems current with the latest security patches and updates
- Install an antivirus solution, schedule signature updates, and monitor the antivirus status on all equipment.
- Develop a security policy that includes but isn't limited to password expiration and complexity.
- Deploy a web filter to block malicious websites.
- Encrypt all sensitive company information.
- Convert HTML email into text only email messages or disable HTML email messages.
- Require encryption for employees that are telecommuting.