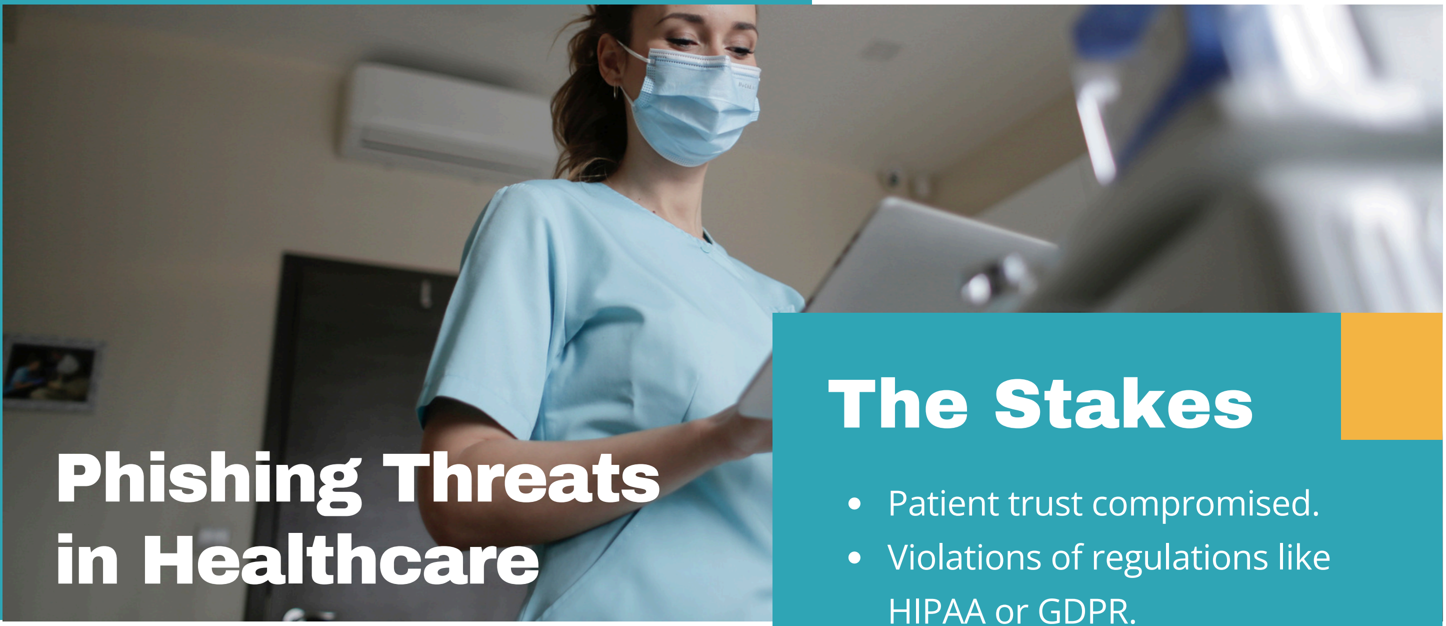
QUICK GUIDE TO AVOIDING PHISHING LINKS

INSODUS TECHNOLOGIES



Phishing Threats in Healthcare

Phishing attacks remain the primary method for launching cyberattacks in the healthcare sector. These attacks often target employees, exploiting trust and urgency to trick them into clicking malicious links or sharing sensitive information.

Why Healthcare is a Prime Target:

- Data Value: Patient data is highly lucrative on the black market.
- Human-Centric Operations: Attackers exploit trust between employees, suppliers, and patients.

Busy Work Environments: High-pressure settings increase the likelihood of accidental clicks.

The Stakes

- Patient trust compromised.
- Violations of regulations like HIPAA or GDPR.
- Significant financial losses due to ransomware or data breaches.

The Numbers*

- Over 80% of healthcare breaches involve phishing.
- Average cost of a phishing-related healthcare breach: $10.93 million (2023).

*Alder, S., 2024. *Average Cost of a Data Breach Rises to $4.88M; Falls to $9.77M in Healthcare*. HIPAA Journal, [online] 31 July. Available at: https://www.hipaajournal.com/cost-healthcare-data-breach-2024/ [Accessed 17 November 2024].

How to Spot a Malicious Link

INSODUS TECHNOLOGIES

5 Key Indicators of a Phishing Link

Suspicious URLs:

- Always hover over a link to preview the URL.
- Watch for subtle misspellings (e.g., medicentre.com instead of mediccenter.com).
- Avoid clicking on shortened links (e.g., bit.ly or tinyurl) unless you're sure of the sender.

Urgent or Threatening Messages:

- Phrases like "Your account will be deactivated" or "Payment overdue—click here to resolve" are common.
- Attackers often create a sense of panic to cloud judgment.

Unexpected Attachments or Links:

- Be wary of links or downloads in unsolicited emails, even if they appear to come from a known contact.
- Confirm authenticity before taking action.

Generic Greetings:

- Messages that address you as "Dear User" or "Valued Customer" are often scams.
- Legitimate senders typically use your name.

Suspicious Senders:

- Check the sender's email address carefully. Fake addresses often include extra characters or slight misspellings (e.g., admin@company-secure.com).

Protecting Yourself from Phishing Links

Actionable Steps to Stay Safe

INSODUS TECHNOLOGIES

Think Before You Click:

- Always pause to inspect links. If in doubt, don’t click—verify with the sender through a different communication method.

Use Multi-Factor Authentication (MFA):

- Even if credentials are compromised, MFA adds a crucial layer of protection by requiring additional verification.

Keep Software Updated:

- Regularly update email clients, browsers, and operating systems to patch vulnerabilities attackers might exploit.

Implement Email Security Tools:

- Use email filtering systems to block phishing emails before they reach your team.

Report Suspicious Messages Immediately:

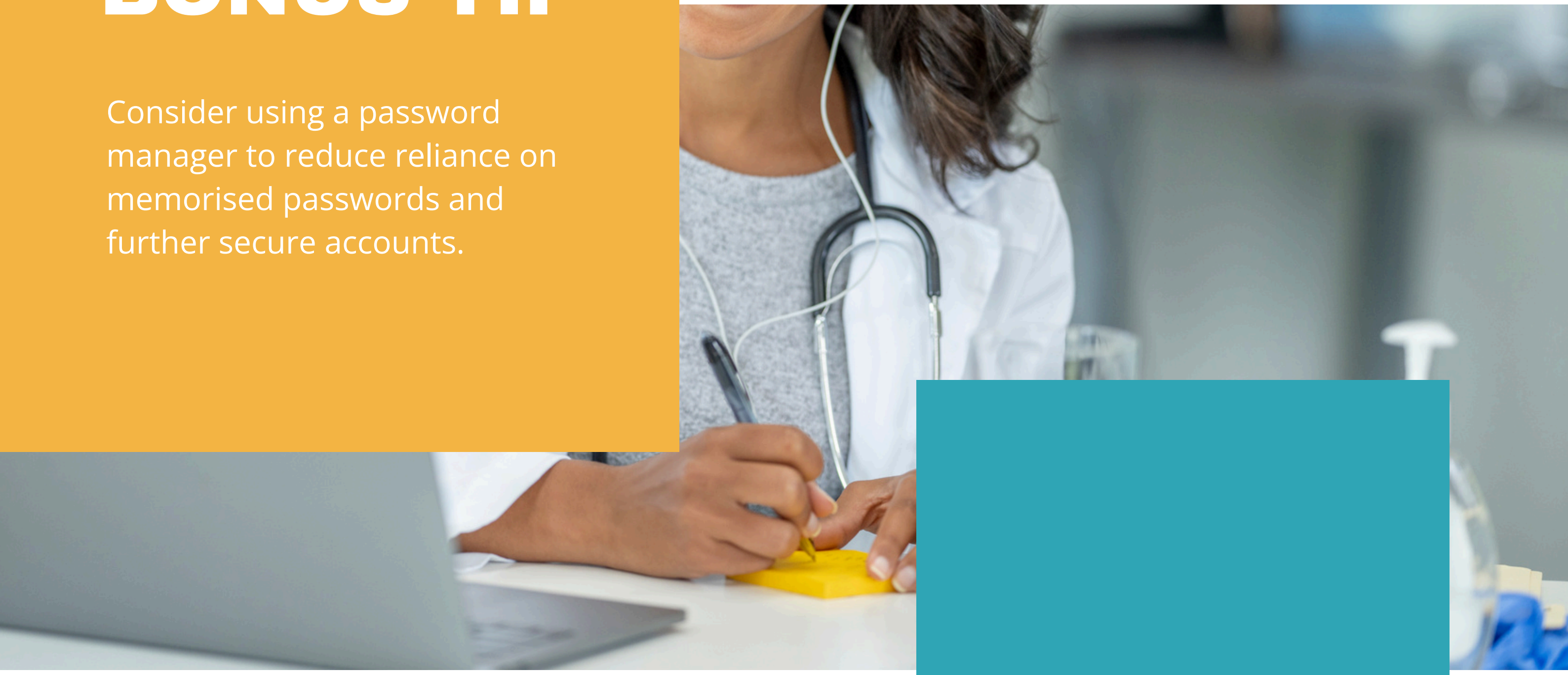
- Create a clear protocol for reporting phishing attempts within your organisation. Fast action can prevent widespread harm.

Conduct Regular Training:

- Host workshops and simulations to teach employees how to identify phishing links and respond appropriately.

BONUS TIP

Consider using a password manager to reduce reliance on memorised passwords and further secure accounts.



Take the Next Step in Cybersecurity

Avoiding phishing attacks is a team effort that starts with awareness and proactive measures. By implementing these best practices, you protect your patients, your data, and your reputation.

For more detailed guidance and tailored solutions, **get in touch today!**

hello@insodus.tech
+372 64 31310