Don’t get phished.

Phishing scams are now one of the most prevalent forms of cybercrime. In fact, most malware threats are spread through emails that contain malicious links or attachments.

To combat phishing emails, it is important to recognize one and protect yourself from it.

What is a phishing email?

A phishing email is a type of scam where cybercriminals send you an email and trick you to divulge any confidential information. The email usually includes a link that takes you to a fake website that looks identical to the legitimate site. For example, if the legitimate site is **paypal.com**, the scammer may use a website address like **pay-pal.com**.

How to recognize a phishing email?

- The sender of the email may impersonate an organization or someone you trust.
- The email often tells a story to manipulate you to click a link or open an attachment in the email.
- The email leads you to a website address that may request details that the legitimate site does not normally ask for. The fake website also does not provide a valid certificate and is not secured with an HTTPS connection.

How to protect yourself from phishing attacks?

- Do not open unsolicited emails from unknown and untrusted sources.
- Do not click links or open attachments from emails that you suspect as phishing attacks.
- Contact the Information and Cybersecurity team at securityincident@meditab.com if you think that you are a victim of phishing.

What are the risks of phishing attacks?

Successful phishing attacks can put the protected data of our clients at risk. The breach of protected data is a violation of the HIPAA policy, which is subjected to proper disciplinary actions.

Key Takeaways

As a medical software company, it is our responsibility to keep our clients' information in safe hands. It is also necessary to comply with and adopt cybersecurity practices to keep our organization safe.

Be careful about the things on the Internet that are too good to be true. Remember, there is no such thing as a free lunch.

Stay tuned for more updates about the Cybersecurity Awareness campaign.