Re: Phishing Attacks – Don't Take the Bait

Today, phishing is the top social engineering attack on businesses, responsible for more than 90 percent of security breaches. We are no exception to this.

Consequently, **everyone needs to remain vigilant to spot phishing**. "Phishing" is the most common type of cyber-attack that affects organizations like ours. These attacks can take many forms, but they all share a common goal – getting you to share sensitive information such as login credentials, credit card information, or bank account details.

Although IT Service Providers maintain controls to help protect your networks and computers from cyber threats, we rely on you and your staff to be our first line of defence. No cybersecurity solution can block 100 percent of attacks. **Please communicate the following to everyone within your organization and make this a mandatory read if possible.**

## Types of Phishing Attacks

We've outlined a few different types of phishing attacks to watch out for:

- **Deceptive Phishing**: In this type of attack, hackers impersonate a real company to obtain your login credentials. You may receive an e-mail asking you to verify your account details with a link that takes you to an imposter login screen, delivering your information directly to attackers.
- **Spear Phishing**: Spear phishing is a more sophisticated phishing attack that includes customized information that makes the attacker seem like a legitimate source. They may use your name and phone number and refer to [COMPANY NAME] in the e-mail to trick you into thinking they have a connection to you, making you more likely to click a link or attachment.
- **Whaling**: Whaling is a popular ploy aimed at getting you to transfer money or to send sensitive information to an attacker via email by impersonating a real company executive. Using a fake domain that appears similar to ours, they look like normal emails from a high-level position (typically the CEO or CFO) and ask you for sensitive information (including usernames and passwords). A few things to watch for:
    - **Doppelgangers**: Whalers may utilize fake e-mail domains that look similar to our domain (@Microsofts.com, @Microsoft-Office1, etc.).
    - **A hurried tone**: Whalers will often ask you to send money immediately, stating that they're busy and can't do it themselves.
    - **E-mail only**: Since whaling relies on impersonating others via a fake address, they will ask you to only reply by email, not phone.

## How to Detect a Phishing Email

- **Suspicious Senders:** Cybercriminals use various spoofing techniques to trick users into believing an email is legitimate. Check the domain closely for close 'cousin' domains. Be cautious when reading email on your mobile device, as only the display name may be visible even if the email is bogus.
- **Subject Lines & Tones:** Enticing, urgent, or threatening language is commonly used to encourage the recipient to take immediate action. Evoking a sense of curiosity, greed, or fear is a common tactic.
- **Greetings:** Phishers often send out mass emails to gather information, so they use generic greetings. But, sophisticated phishers personalize their emails with names, email addresses, and even breached passwords.
- **Errors:** Read the email carefully. Grammatical errors are an obvious red flag, but sophisticated hackers do not make glaring errors. Instead, there may be more subtle mistakes, such as minor spacing issues or use of symbols instead of words. In some cases, there will be no errors.
- **Links:** Before clicking, hover over the link to see the URL of where the link actually leads, and beware of link shorteners, such as Bitly or TinyURL. Keep in mind that phishing emails can include clean URLs in addition to the phishing URL to trick users and email filters.
- **Attachments**: Be wary of emails that include attachments. Phishing emails may include a link in an attachment, rather than the body of the email, to avoid detection by an email filter.
- **Images**: Cybercriminals can easily replicate brand logos, images, and badges in emails and webpages that are indistinguishable from the real thing. Consider all the above factors as you decide whether to click.

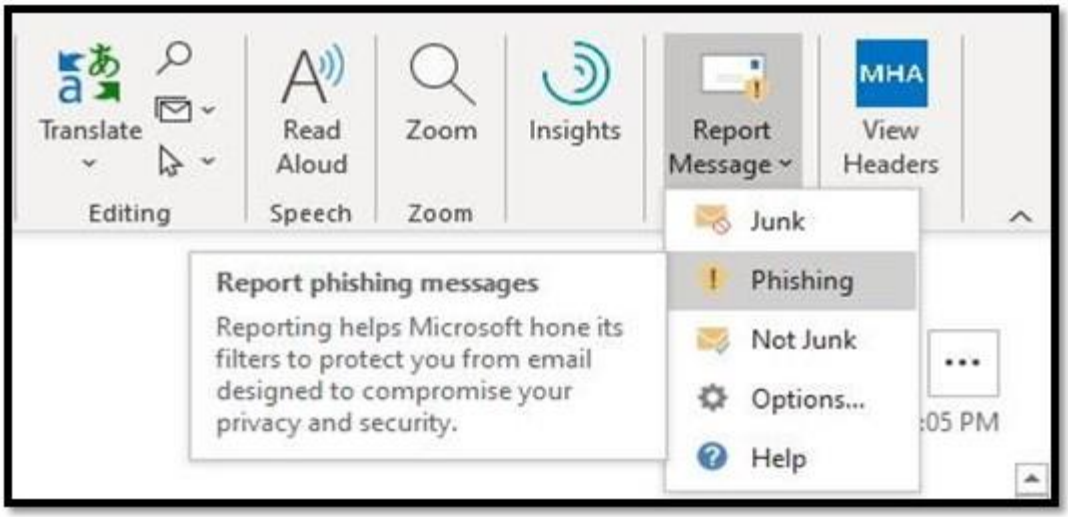
## What You Can Do

To avoid phishing schemes, please observe the following best practices:

- Do not click on links or attachments from senders you do not recognize. Be especially wary of .zip or other compressed or executable file types.
- Do not provide sensitive personal info, usernames, or passwords via email.
- Do not try to open any shared document you're not expecting to receive.
- If you cannot tell if an email is legitimate, please let us know ASAP. Do NOT attempt to investigate further or click on any of the links within the email.
- Be especially cautious when opening attachments or clicking links if you receive an email containing a warning banner (similar to below) indicating that it originated from an external source.

## Reporting Suspected Phishing Messages

For those email accounts under Microsoft Office 365, you can also report a message as **"Phishing"** using the **Report Message** Feature available in the top right of the Outlook client. This will tag the email as Phishing.




Once you submit, you should see this confirmation message and the email will be deleted from your Inbox:


Don't know where to start? Let us walk you through our security solutions and answer any questions you may have. The cybersecurity experts at ZTek Solutions can help. We offer comprehensive security services that can help improve your security posture and protect your business. These include but not limited to the following areas:

- Firewall Network with Security Services
- Endpoint Security Services
- Managed Detection and Response
- Advanced Email Security Services
- Security Awareness Training
- Dark Web Monitoring
- Disaster Recovery & Backup Solutions