Your journey, secured.

Lateral Phishing

Spotting the Threat

The email threats faced by organizations today vary greatly in complexity, volume, and impact. Here we take a closer look so you can spot the threat before it harms you or your organization.

With lateral phishing attackers send phishing emails from hijacked accounts to contacts within and outside of the company to spread the attack more broadly.

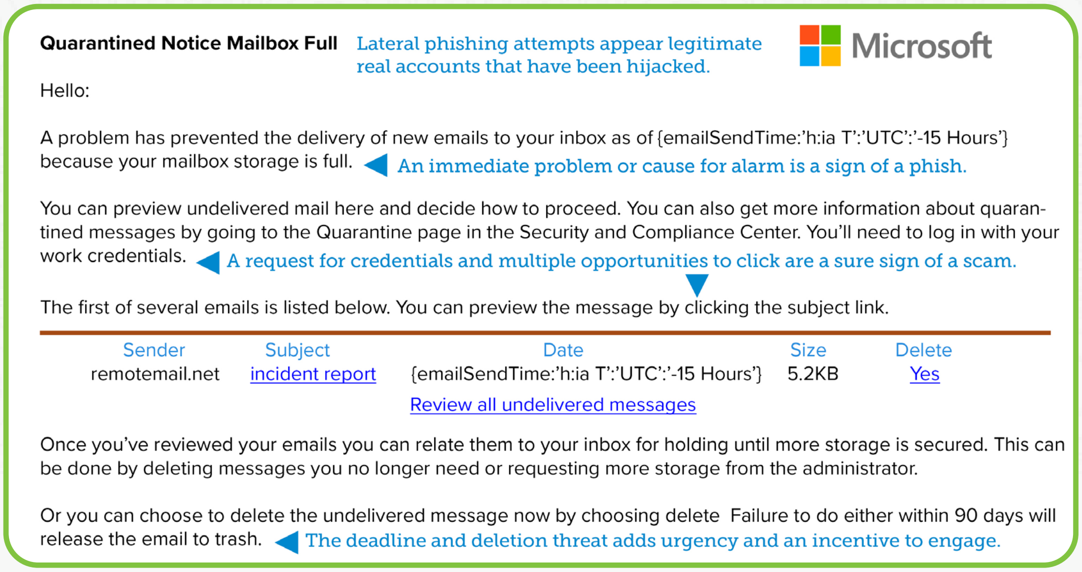
Because these attacks come from a legitimate email account and appear to be from a trusted colleague or partner, they tend to have a high success rate.

Despite these facts, targets can prevent lateral phishing from succeeding by:

- Being skeptical of emails from partners that are written in a different tone or style.
- Being wary of any requests for financial or confidential information.
- Verifying the sender's identity with a phone call.
- Having a manager or colleague weigh in if you're unsure.
- Alerting your IT team if you suspect anything suspicious as it could be part of a larger attack.

The sample shown highlights an example of lateral phishing.

Example



Quarantined Notice Mailbox Full Lateral phishing attempts appear legitimate real accounts that have been hijacked.

Microsoft

Hello:

A problem has prevented the delivery of new emails to your inbox as of {emailSendTime:'h:ia T':'UTC':'-15 Hours'} because your mailbox storage is full. ◀ An immediate problem or cause for alarm is a sign of a phish.

You can preview undelivered mail here and decide how to proceed. You can also get more information about quarantined messages by going to the Quarantine page in the Security and Compliance Center. You'll need to log in with your work credentials. ◀ A request for credentials and multiple opportunities to click are a sure sign of a scam.

The first of several emails is listed below. You can preview the message by clicking the subject link.

Sender	Subject	Date	Size	Delete
remotemail.net	incident report	{emailSendTime:'h:ia T':'UTC':'-15 Hours'}	5.2KB	Yes

Review all undelivered messages

Once you've reviewed your emails you can relate them to your inbox for holding until more storage is secured. This can be done by deleting messages you no longer need or requesting more storage from the administrator.

Or you can choose to delete the undelivered message now by choosing delete Failure to do either within 90 days will release the email to trash. ◀ The deadline and deletion threat adds urgency and an incentive to engage.