A Phishing Story

The
Bait

From: Help Desk <support@insidevideo.it>
Sent: February 6, 2022 06:05
To: <*professor*@senecacollege.ca>
Subject: Mailbox Storage Alert

[EXTERNAL EMAIL] Please take caution when clicking links, opening attachments or responding to requests for information.

Your mailbox storage has reached 98% on the email server.Visit OutlookStorage Access Page and login to adjust and maintain your Mailbox storage.

At 100% limit, these email features:
· Sending messages
· Receiving messages
· Forwarding messages

Will not be available for your utilization.

IT Help Desk

What are all the red flags?

Seneca's help desk is
Service Desk <servicedesk@senecacollege.ca>
not Help Desk <support@insidevideo.it>

Seneca's help desk is *not* EXTERNAL EMAIL.

"Your mailbox storage has reached 98% on the email server.Visit OutlookStorage Access Page and login to adjust and maintain your Mailbox storage."

"on the email server" – where else would my mailbox be?
"server.Visit" no space after period

Hover mouse cursor over link to check but destination is masked by
https://protect-us.mimecast.com/s/-fTaCYEBq4T8qgyXu0Sl6-
?domain=2af1e518.sibforms.com
– should have looked at the From address.

<div style="border:1px solid black; padding:1em;">

The Hook

Doing four things at once
- Email – unexpected
- Marking – behind on that
- Course content revisions: slides, assignment instructions, quiz revisions
- I should be doing three other things but I've forgotten what they are.

Stressed
- Have had one weekend and 1 day off in over a month

Panic
- Have no time for administrative PITA tasks
  - Spent 5 hours doing that on Friday
  - There are only two working days between Friday and Monday – not enough to keep Monday to Friday tasks up to date.
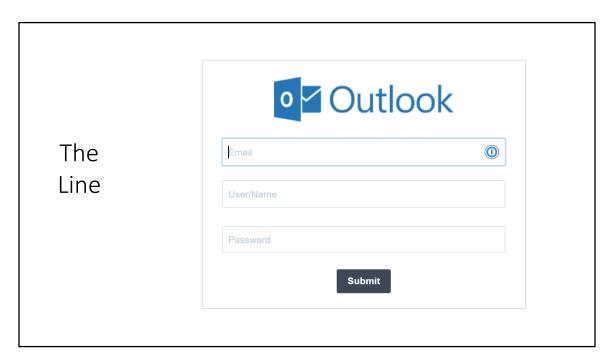
No worries: mimecast.com
  - "Mimecast's value begins with the most effective cloud-native platform for the #1 threat vector: email."
  - "Targeted Threat Protection helps establish a foundation for enterprise-wide resilience, helping to deter everything from ransomware to impersonation."

</div>

mimecast.com does not do what you think it is supposed to do, that is *prevent* phishing emails and *disable* malicious links.
What *does* it do?
Hides strange URLs behind even stranger URLs.
Takes seconds longer to reach the real URL so it is easy to stop paying attention.

The Line

Yet another indecipherable URL but the sibforms.com domain has nothing to do with me or Seneca.
Yet, with so many services now being in the cloud, how do I know where ITS is hosting things?
IT Help Desk (sibforms.com)
https://2af1e518.**sibforms.com**/serve/MUIEAAwGtS84rIUQhoMcVjk1fCxjgsaatlnmJrV
Vhfs6kVy7ajfvfDqNYt9eba1JOIaWK_zUYOQ3_RxdjNPjXvLh3zTIJurl89Slzntm7EyxlhV9q
-ohiicPK-
PJLTkTRV27ZBCGUZQlOg30dOUyrjRcCb0drQ_jc6n7ApGoaaHRgEW1yOAk43UpDl04vO
g4fIF6Cfyx3qBzwFd

Outlook icon is a bit fuzzy.
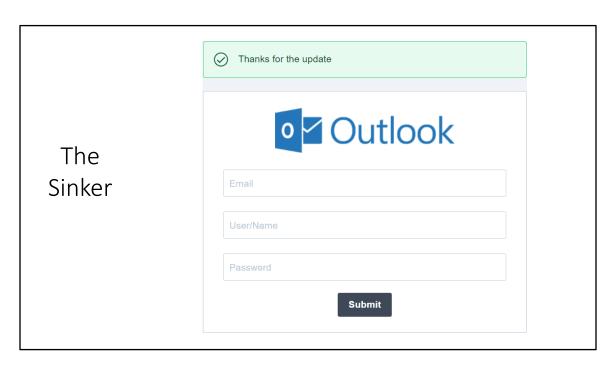Why "User/Name"? Email address is usually user id.
But User/Name can be the administration account for multiple email accounts on the server.
In the past, there were some Seneca systems accepting *only* the Username (in front of @) and some requiring the full email even though the system knows the user is *inside* the firewall and the target system is *within the SenecaCollege.ca domain* so full email is redundant.

Have macro scripts to spit out email address and password (I know, I shouldn't, but I do anyway because…see above and previous slide)
and being so used to pressing Enter, let's just get this over with.
Wait, I just saw the password was reflected in plain next…nnnooooooo

The
Sinker

"Thanks for the update" ?!?!?!
Wait, this needed maintenance to clean out old emails and huge attachments.

Aw, SNAP.

Well, its about time password should be changed anyway.
MFA already on the account so sign in impossible without it.