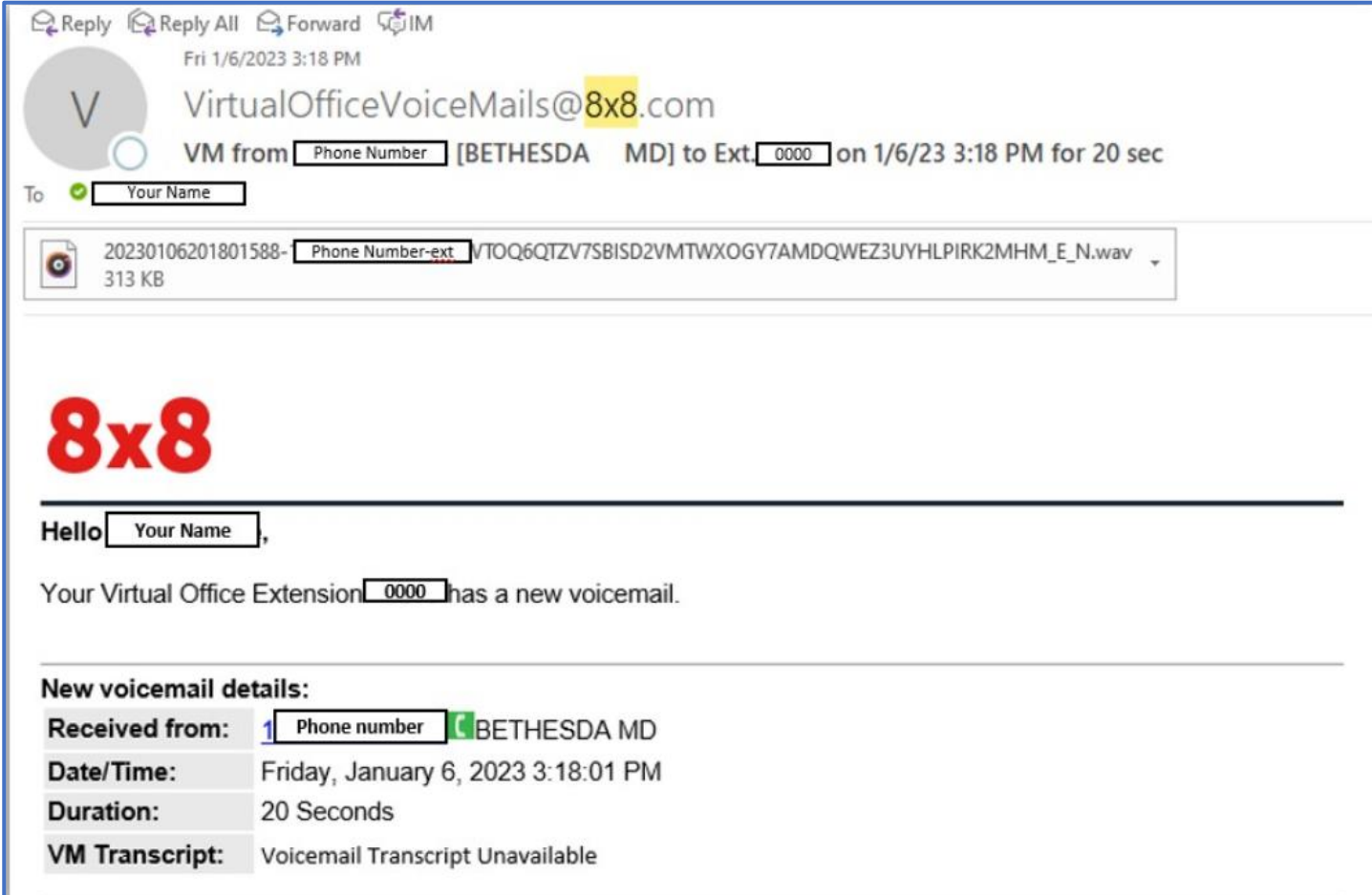


The Office of Information Technology (OIT) recently completed a simulated phishing scenario titled, *employee.name@montgomerycollege.edu 2 missed VN on 01/26/2023*. The voicemail email scenario directed the recipient to click a link and then enter a password in order to listen to a message.

Voicemail phishing emails are successful because they often spoof legitimate brands to look like a typical office communication and imply a sense of urgency. Content can be very generic, making it difficult for the user to discern the sending voicemail system.

### Familiarize yourself with MC's voicemail system:

- Sender is: VirtualOfficeVoiceMails@8x8.com
- Sample subject format is:  
VM from 123 456-789 [City ST] to Ext. 1234 on 01/06/2023 3:18 PM for 20 sec
- MC'S 8x8 voicemail email notifications do **NOT** require employees to login to hear voicemail audio messages.
- Any other voicemail email received, purported to be legitimate, is fraudulent if it does not follow the guidelines above.
- **REPORT** the email! Do not click on the link to investigate on your own.
- Check out the sample voicemail email below for reference:



The screenshot shows an email interface with the following elements:

- Buttons: Reply, Reply All, Forward, IM
- Date and Time: Fri 1/6/2023 3:18 PM
- Sender: VirtualOfficeVoiceMails@8x8.com
- Subject: VM from [Phone Number] [BETHESDA MD] to Ext. [0000] on 1/6/23 3:18 PM for 20 sec
- To: [Your Name]
- Attachment: 20230106201801588-[Phone Number-ext]-VTOQ6QTZV75BISD2VMTWXOGY7AMDQWEZ3UYHLPK2MHM\_E\_N.wav (313 KB)
- Logo: 8x8
- Greeting: Hello [Your Name],
- Message: Your Virtual Office Extension [0000] has a new voicemail.
- Section: New voicemail details:
- Received from: 1 [Phone number] [BETHESDA MD]
- Date/Time: Friday, January 6, 2023 3:18:01 PM
- Duration: 20 Seconds
- VM Transcript: Voicemail Transcript Unavailable

**Good news: 883 employees reported** the phishing scenario to the Phishtrap. **Nice work MC!**

**Opportunities for improvement: 407 employees clicked the link within the training email; of these individuals, 77 entered their credentials.**

**Did you click?** In a real-world phishing attack clicking the link may have prompted you to give up your login credentials.

Review the red flags within this type of phishing attack and to learn ways to spot a suspicious email:

The image shows a screenshot of an email interface with several red callout boxes pointing to suspicious elements:

- Unknown sender and domain:** Points to the 'From' field: Alerts <aler1@premiumisp.net>
- No name; vague content:** Points to the 'Subject' field: First.name @montgomerycollege.edu 2 missed VN on 01/26/2023
- Hover over the link to show URL Unknown web address:** Points to a link in the email body: <https://docs.premiumisp.net/s/vbm3ocpm44remipazc/5f5547/9a7fa6d3-b6ae-45f5-9339-b1522252cdd6/>
- Link leads to fake M365 themed log in page!** Points to a screenshot of a fake 'Sign In' page with a 'Sign In' button.
- Note: MC's voicemail system is 8x8!** A red box at the bottom states: **MC's 8x8 email notifications do NOT require employees to login to hear VM audio messages**

### What should you do if you suspect an email may be a phishing attempt?

Let IT Security analyze the email for you - **REPORT** the email! The Report Phishing button within your email client allows you to quickly report suspicious emails to IT Security. [Learn how to access the Phishing Reporter button when using Office 365 at home.](#) If you accidentally clicked on a link or attachment in a suspicious email, contact the [IT Service Desk](#) immediately.

Follow these additional tips to avoid phishing scams:

- Question any email request that is asking for your login credentials.
- Check your emotions. Do not be curious and investigate the link – **REPORT the email.**
- Always verify! If you know the sender, but the email seems out of context, follow up with a quick phone call.