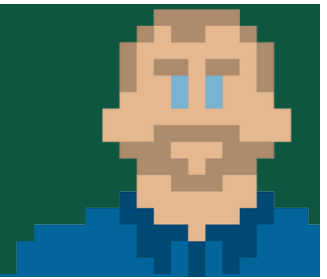




UNIVERSITY of WISCONSIN
GREEN BAY

WANTED

BY UWGB IT SECURITY



Conspiracy to Commit Computer Intrusions; Conspiracy to Commit Wire Fraud

Uwgb Support <no-reply.Uwgb@**dins.jp**>

Wed 7/10/2019 1:50 PM
Phoenix, Phlash

Voice-10-July2019wa.**.htm**
3 KB

Microsoft

Hello Phoenixp,
You missed a call from +1 (502) 502-5264
Note: ****This is an automated message and need immediate attention please do not reply****

- Suspicious address
- “.htm” attachment in voicemail
- Inappropriate branding
- Unreasonable urgency, incorrect grammar

COMMON PHISHING PLOYS

Suspects are skilled in the use of disguises and have been known to imitate the following:

VOICEMAILS	DOCUMENTS	IT DEPARTMENT
------------	-----------	---------------

Genuine UWGB voicemail notifications will not...

- Come from any address that doesn't end in "@voicemail.uwgb.edu"
- Contain links
- Contain attachments ending in ".htm" or ".html"
- Have Microsoft, Office 365, or OneDrive branding
- Require you to sign in

Don't trust documents (shared or attached) that...

- Were provided to you with little or no explanation
- Claim to be an invoice that you weren't expecting to receive
- Ask you to enable macros (ever!)
- When previewed, contain only a link to a document hosted on a cloud service

UWGB IT will never...

- Ask you to sign in in order to "confirm" or "validate" your account
- Threaten to permanently close your account
- Ask you to give them your password
- Reach out to you from an email address that doesn't end in "@uwgb.edu"

Phishing messages are likely to be armed with malicious links or attachments and should be considered dangerous. If spotted, they should be forwarded as an attachment to

ABUSE@UWGB.EDU