

The Anatomy of a Phishing Attack

The report that installed itself

UMass Boston Information Security Office • 7 min read

Kurt Sooknanan • Keyshawn Jeannot • Lynn Constant • Joseph Singletary • Thalyta Andrade

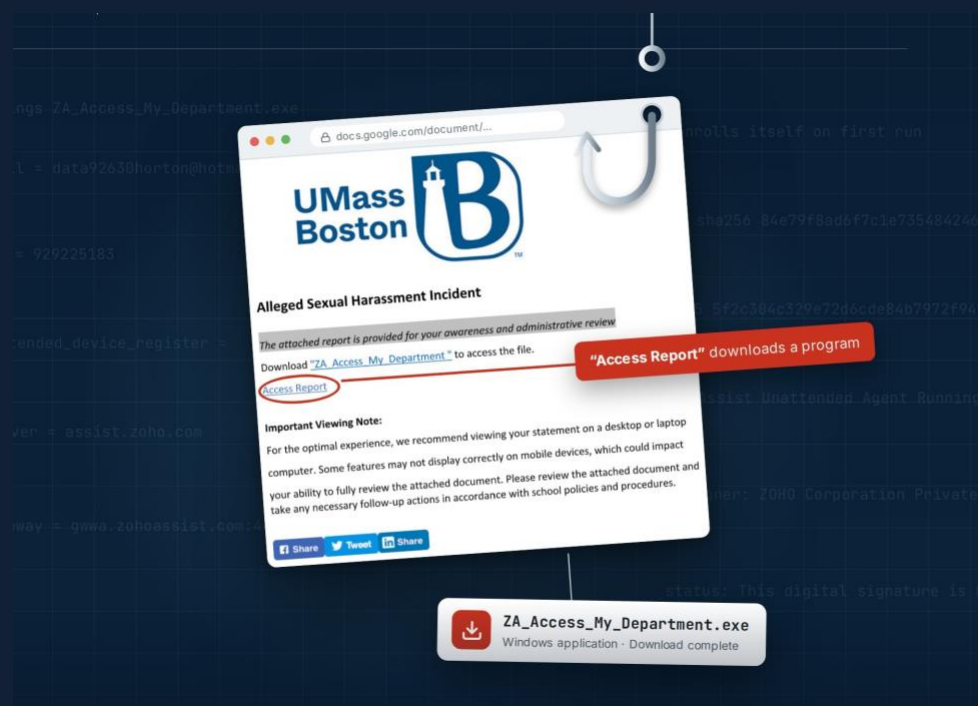


Figure 1. The page a UMass Boston recipient was sent to. The logo is ours. The page is not.

No attachment

The “report” was a link to a download.

A clean scan

The file was signed by a real company.

No warning

Nothing on screen once it worked.

It never asked for a password.

No fake login page. No request to “verify your account.” This one asked for something far more ordinary: to be opened. The click did the rest.

What follows is a real phishing attempt (a scam email dressed up as something you can trust) against the UMass Boston campus community. This phishing attempt was traced from the moment it landed in an inbox to the moment a stranger could take control of the computer.

The short version

From inbox to remote control

A message sent from a genuine @umb.edu address told recipients that the Student Services Office had shared a report about an alleged sexual harassment incident. The link opened a real Google Doc dressed in UMass Boston branding. Its “Access Report” button did not open a report. It downloaded a Windows program: a genuine copy of Zoho Assist, real software that IT help desks use to control computers from a distance.

Hidden in that program’s settings was an outside account. Run it, and the computer quietly signs itself up to be controlled from afar, with no one asked and no one watching. That hands a stranger the screen, the keyboard, and everything the user’s account can reach. The same page, with only the logo swapped, also reached the University of Michigan. This was a campaign, not a one-off.

BOTTOM LINE

A document you have to install is not a document.

The attack never needed a password. One click on a real program from a real company was enough.

Attack timeline

Five steps

Five steps. The only one you can stop is the third.

1. Email from a name you know
2. Link to a real Google Doc
3. Download is a program
4. Running it hands over the computer
5. A stranger takes control



Figure 2. Five steps. The download a program is the only step you can stop.

Step 1 · The email

It Came From Inside

The first thing to understand about this message is where it came from: a genuine university address. Either the account behind it had been stolen, or the sender's name was faked well enough to pass. Both roads lead to the same place; an email that looks like it belongs.

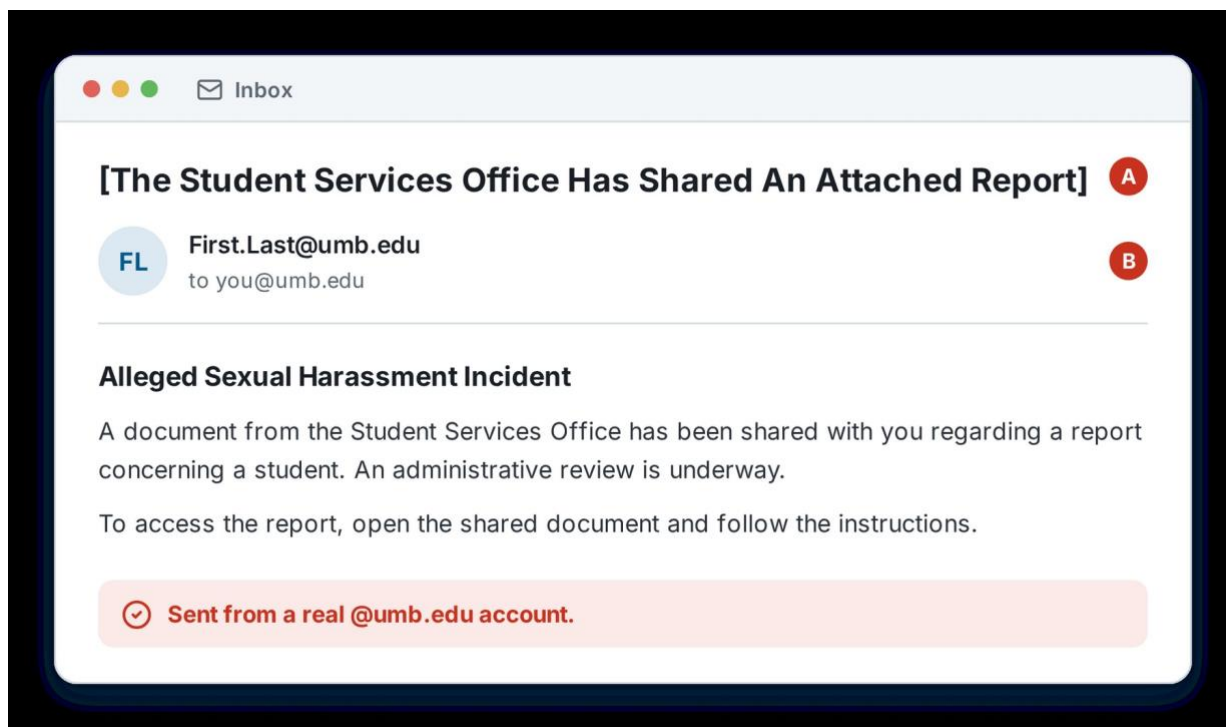


Figure 3. The message, as it appeared in the inbox.

Why the subject works

Harassment. A review. Records. The topic is uncomfortable enough that most people open it fast and quietly, without asking a colleague whether they actually sent it.

Why the sender works

Stolen accounts send mail that passes every spam and security filter, because the mail really is coming from a UMass Boston account. Nothing about the sender looks wrong.

A familiar name is not proof. Accounts get stolen.

What a university will never do

- Spring a case or review on you that you have never heard of.
- Ask you to install software to read a document.
- Tell you to click “Yes” on a Windows security warning.
- Ask you for your username and password.

Step 2 · The lure

The Link Opens a Real Google Doc

Click the link and you do not land on some suspicious website. You land on Google. Putting the trap on Google's own site gets it past spam filters and makes the next click feel routine. Look closely, though, and five things on the page give it away.

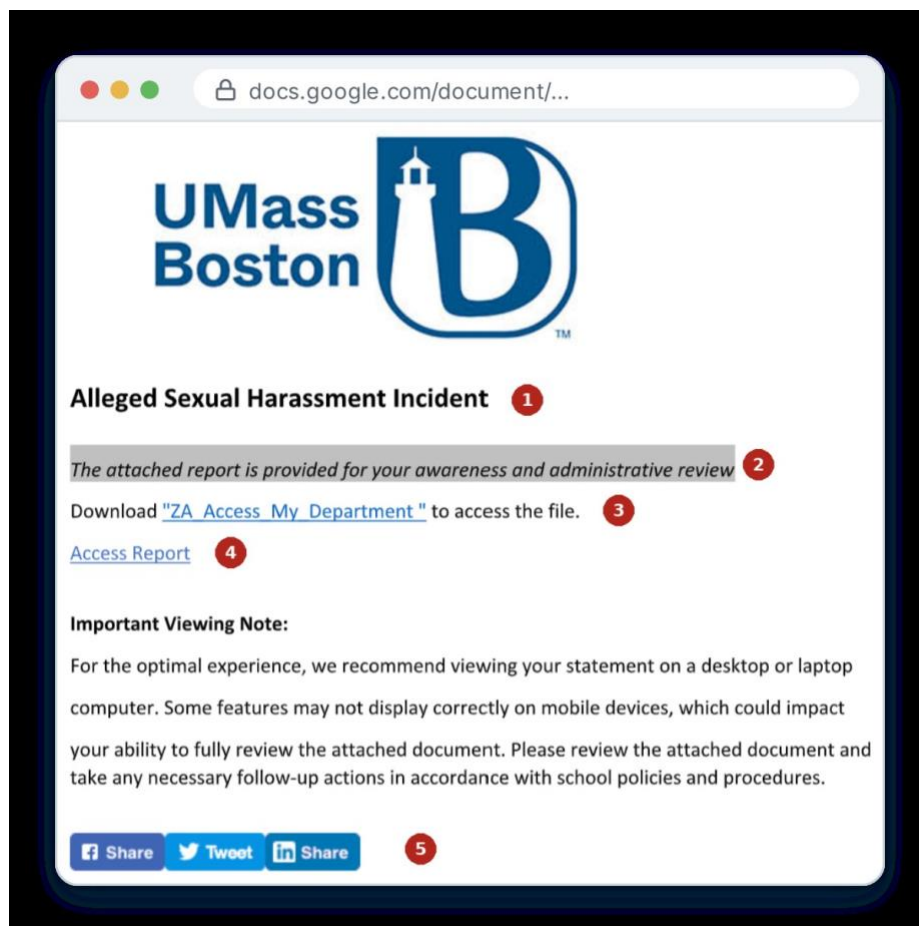


Figure 4. The lure page. Each red marker is a giveaway.

Five giveaways

6. A subject you will not question. A topic this sensitive makes you less likely to check with anyone.
7. Official-sounding filler. "Administrative review" gives the page an authority it does not have.
8. A file name, not a document. Real shared documents open right in your browser. You never download them.
9. "Access Report" is a download button. It delivers a Windows program, not a report.
10. Share buttons on a private report. Nobody shares a confidential report on Facebook. The buttons were copied from a public web page.

A document you have to install is not a document.

Step 3 · The download

The Report Is a Program

This is where the story turns. The button downloaded a Windows program. It carried a real company's digital signature, and the first virus scan came back clean.

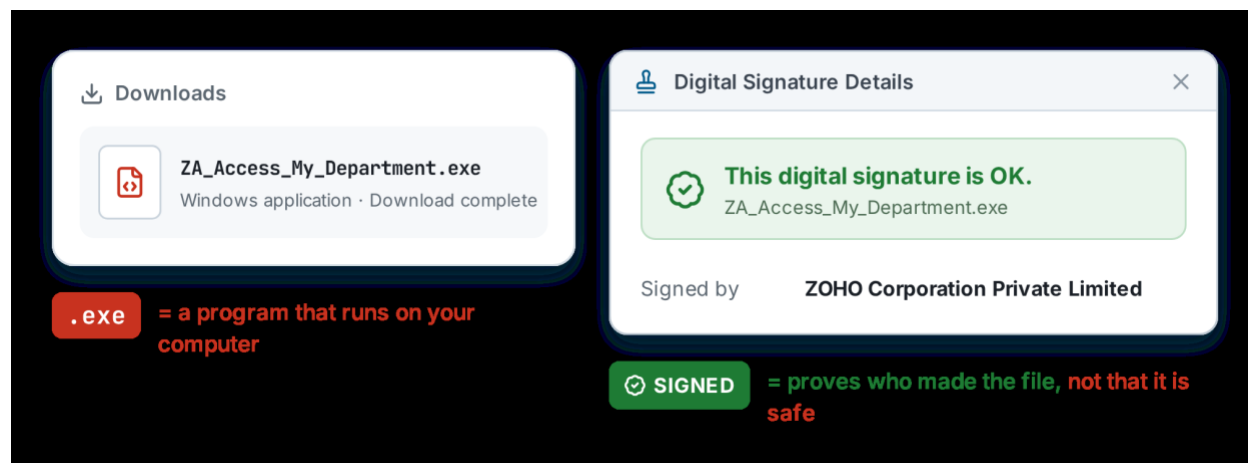


Figure 5. The signature is genuine. So is the software.

Real software, borrowed

The download is Zoho Assist, a real product that IT help desks use every day to fix computers from a distance. Nothing about the file is fake.

That is exactly why the virus scan came back clean. Antivirus does not flag a genuine, signed product that thousands of companies use on purpose.

NO ANTIVIRUS FLAGGED THIS FILE

Our analysts tested it on a sealed-off, throwaway computer (a “sandbox”). It was never run on a university or personal device.

A clean scan is not a safe file. The attack is not the program. It is the settings hidden inside it.

The lesson is bigger than one file:

Attackers stopped writing malware.

They ship real tools instead.

What the message told people to do next

“Click Next. Select I Agree. Let the installation finish.

If Windows asks for permission, choose Yes. Any prompts are part of the normal process.”

Paraphrased from the campaign text published by other universities.

Read that again. The warning you were about to see was explained away before you saw it.

Step 4 · The install

What Happens If You Run It

The installer runs like any other. Then it says the quiet part out loud.

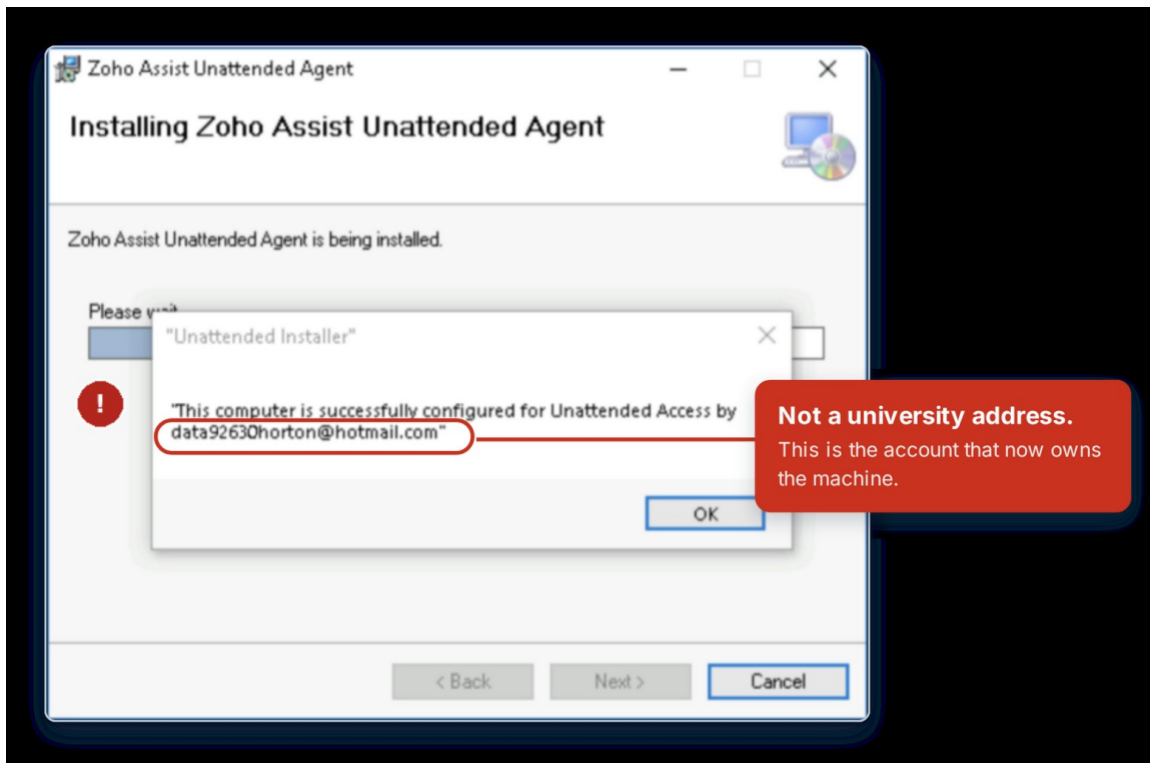


Figure 6. The confirmation names the account that now owns the machine. It is not a university address.

Source: safecomputing.umich.edu/phishing-alerts

“Unattended” means no pop-up, no window, and no way for you to tell it is happening.

Normally, a support technician has to ask for your permission, and you watch everything they do on your screen. This version skips both. It hides in the background, starts every time the computer turns on, and waits.

Step 5 · The hidden catch

What Was Hiding Inside

The installer already knew who it would report to. Someone else’s account was written into the file before it was ever sent. Pull the readable text out of the program, and there it is.

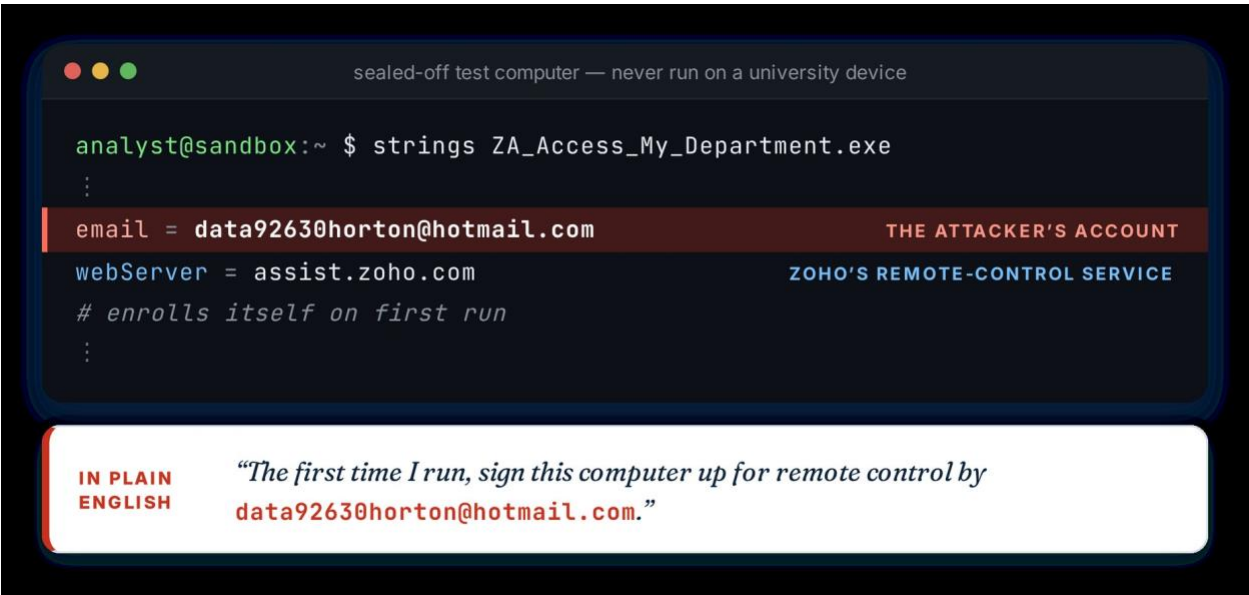


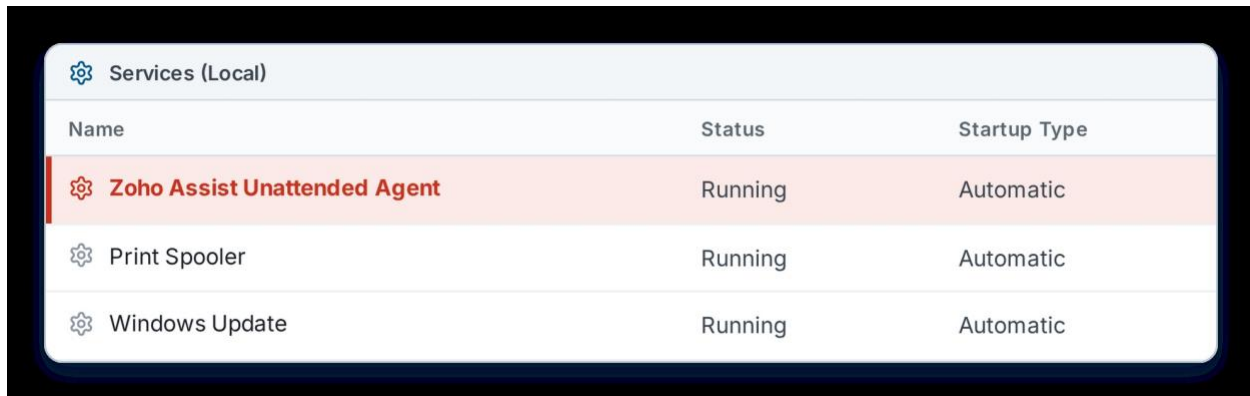
Figure 7. The attacker’s account is built into the installer before you ever click.

What the stranger gets

Table 1. Access available to the stranger

Access	What it means
Your screen and keyboard	Live control, whenever the machine is on.
Saved passwords	Everything the browser remembers for you.
Your logged-in accounts	Everything you’re signed into. No password or phone approval.
Files and email	Anything the account can open.
The campus network	Shared drives and university systems your account can open.

One install replaces every password you have.



Name	Status	Startup Type
 Zoho Assist Unattended Agent	Running	Automatic
 Print Spooler	Running	Automatic
 Windows Update	Running	Automatic

Figure 8. One line in a list of background programs. That is the only trace it leaves on the computer.

The bigger picture

Same Page, Different Logo

This is a campaign, not a one-off. The same page was sent to other universities with the branding swapped out.

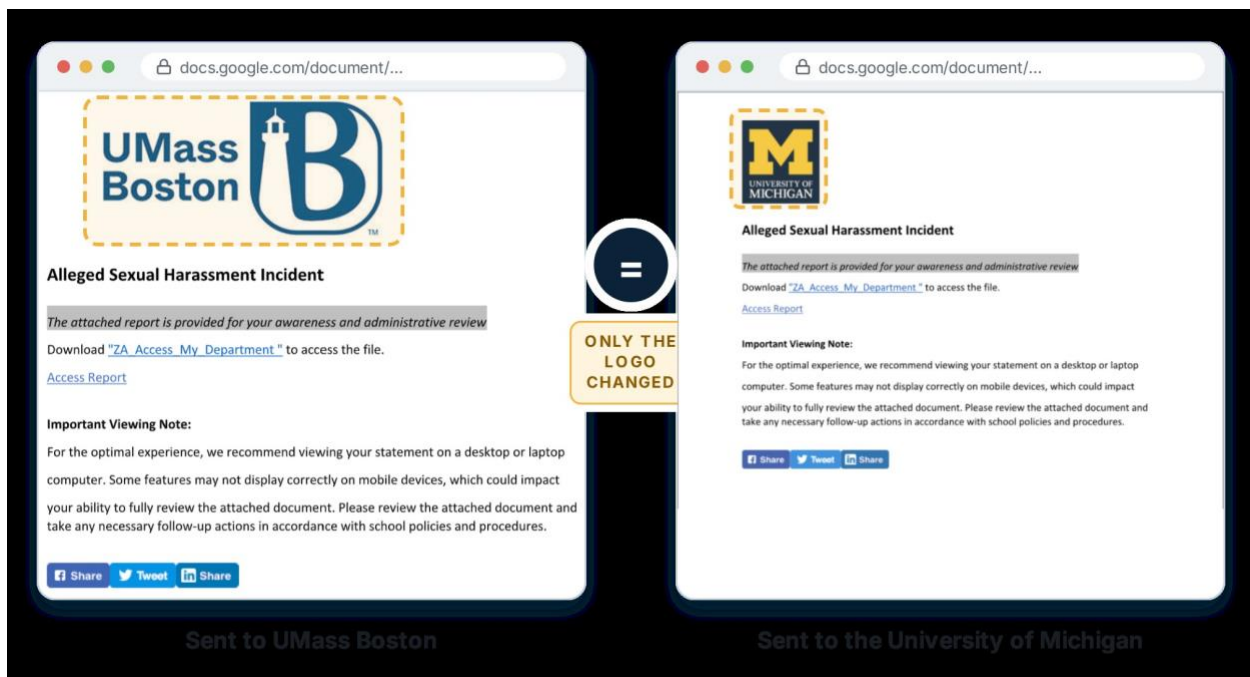


Figure 9. The same phishing page sent to two universities with different logos.

On August 19, 2026, Michigan published an alert about it, naming the same file and the same Student Services Office story (safecomputing.umich.edu/phishing-alerts).

The wording is disposable. The trick is not.

What to do

Five Signs, Every Time

- An attachment that is really a link.
- A “document” that downloads a program: files ending in .exe, .msi, .scr, .dmg
- Instructions to click through installation pop-ups. Real documents never need this.
- A subject that makes you want to handle it alone.
- A case or review you were never told about.

VERIFY

Check with the sender another way.

Call them, or message them somewhere other than a reply. A stolen account will happily answer the reply.

If it already happened

If You Already Ran It

1. Disconnect from the internet. Turn off Wi-Fi or unplug the network cable. Do not uninstall it first. That destroys evidence and does not remove the access.
2. Change your password from another device. Then change any other account you signed into on that machine.
3. Email the Information Security Office. That machine needs to be looked at, not cleaned up and handed back.

Nobody is in trouble for clicking. The only thing that makes it worse is waiting.

Words to know

Plain-English Glossary

Phishing

A message that pretends to come from someone you trust, so you will click, open, or share something.

Malware

Software built to harm or spy on you. This attack did not need any: it used a real product instead.

Remote-support tool

Software that lets another person see and control your computer over the internet. IT help desks use it every day.

Unattended access

Remote control that works without anyone at the computer approving it or seeing it happen.

Digital signature

A tamper-proof stamp that shows who made a file. It proves where a file came from, not that it is safe.

.exe file

A Windows program. Opening one runs code on your computer.

Sandbox

A sealed-off, throwaway computer that security teams use to open suspicious files safely.

Indicator

A clue, such as a file fingerprint or web address, that helps IT spot the same attack elsewhere.

Appendix • For IT staff

Indicators

Table 2. Technical indicators associated with the phishing campaign

Indicator	Value
File	ZA_Access_My_Department.exe
SHA-256	84e79f8ad6f7c1e73548424625206c861289c4c31b051e0b3f9c6673329da7cd
MD5	5f2c304c329e72d6cde84b7972f94973
Enrollment address	data92630horton@hotmail.com
Zoho org_id	929225183
Network	assist.zoho.com · gwwa.zohoassist.com · wa5.zohoassist.com · *.zohoassist.com

Report it

If you receive a suspicious email, are targeted with a phishing attack, or think you may have fallen for one, email the Information Security Office with as much detail as you can. Forward the message as an attachment if your mail client offers it.

Abuse@umb.edu