

Cybersecurity Awareness Month

Stay connected, stay safe, stay smart!

1

Avoid Phishing Emails

- Never submit your passwords on Google Forms
- Don't share your personal or financial information
- Beware of fraudulent job offers, gift cards, or calendar invites
- Ignore scare tactics like account deactivation emails
- Don't click on unexpected attachments or links

2

Fraudulent DUO Push

- Do NOT Approve It
- Deny the Request
- Change Your Password

3

ClickFix Popup Window

- Don't copy and paste any command the pop-up suggests
- Close the suspicious window or tab immediately
- Disconnect from the internet after pasting fraudulent command

Report all phishing and fraudulent emails to
security@umbc.edu

doit.umbc.edu/security



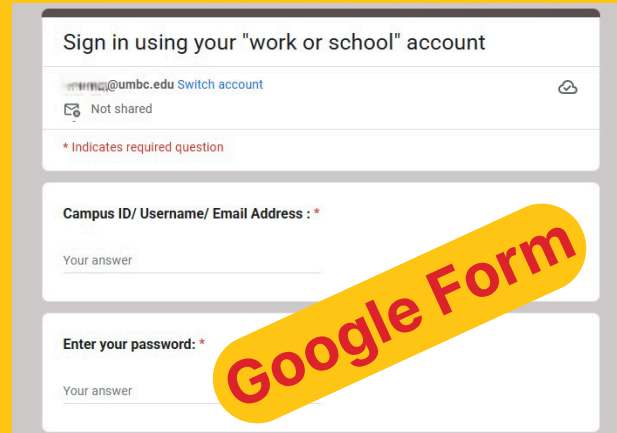
Cybersecurity Awareness Month
DIVISION OF INFORMATION
TECHNOLOGY (DoIT)

Avoid Phishing Emails

You can protect your account by recognizing and reporting phishing emails!

Phishing

Deceives individuals into providing personal information or passwords through malicious links via email.



Sign in using your "work or school" account

umbc@umbc.edu Switch account

Not shared

* Indicates required question

Campus ID/ Username/ Email Address : *

Your answer

Enter your password: *

Your answer

Google Form

Examples

1. Google Forms requesting usernames and passwords
2. Fraudulent job offers or unsolicited gift cards
3. Fake account deactivation notices
4. Unexpected calendar invitations

All Email recipients of University Of Maryland Baltimore County to be a part of this amazing offer. This is a part time job that will not affect your present employment or study at the campus & you'll be working from home. It's fun, rewarding, and flexible.

2-3 hours daily
3 Times needed weekly
Five Hundred And Fifty Dollars (\$550)
Part-Time Job.

To apply, Be sure to visit the link below while M...
you for more info.

[Apply Here](#)

University Of Maryland Baltimore County

Job Offer

Report

Report by forwarding phishing emails to security@umbc.edu.

Your Microsoft account with umbc.edu has been added to the list of accounts that are scheduled to be closed as an inactive students so it is advisable that you confirm this request; if you see this as a mistake please kindly adhere to your umbc.edu email right automatically re enroll into our **SYSTEM** and prevent deactiv

Notice

NOTE: Failure to put your password or an incorrect password will automatically be removed from the **IT HELPDESK** System.

doit.umbc.edu/security



Cybersecurity Awareness Month

DIVISION OF INFORMATION TECHNOLOGY (DoIT)

Fraudulent DUO Push Notification

Use Duo MFA for myUMBC!

If you receive a Duo push notification, including SMS texts or phone calls that you did not initiate:

- Do NOT Approve It
- Deny the Request
- Change Your Password



MFA for All!

Turn on MFA for every online account or application that offers it. This prevents anyone but you from logging in, even if they know your password.

Report all fraudulent Duo pushes to
security@umbc.edu

doit.umbc.edu/security



Cybersecurity Awareness Month

DIVISION OF INFORMATION
TECHNOLOGY (DoIT)

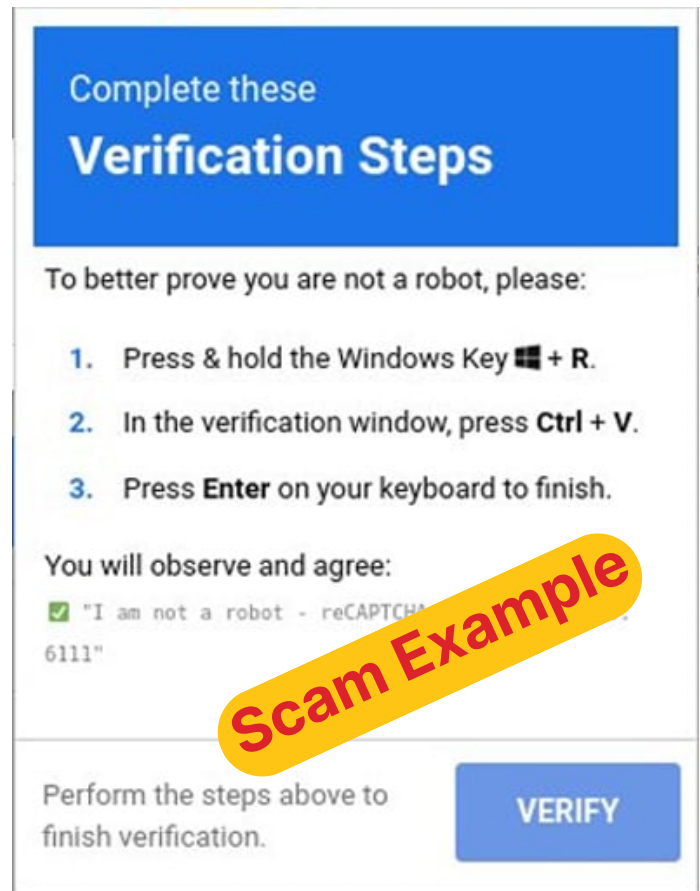
ClickFix Scam

Never copy commands into the terminal!

Beware of this new technique:

This new technique disguises itself as an error message or system alert that looks like it comes from your operating system.

- Never paste commands from a pop-up window or website.
- Close the window or browser tab immediately.



React Quickly!

- Report the incident to security@umbc.edu.
- If you have already entered a command, disconnect from the internet and stop using your device.

Report all ClickFix Scams to
security@umbc.edu

doit.umbc.edu/security



Cybersecurity Awareness Month
DIVISION OF INFORMATION
TECHNOLOGY (DoIT)