Division of Information Technology

Spring 2026

Cybersecurity Newsletter

WELCOME FROM THE CHIEF INFORMATION SECURITY OFFICER!

Hello UMBC, and welcome to DoIT's first bi-annual cybersecurity newsletter! This opening edition is part of a brand new initiative aimed to engage, educate, and inform the campus community about relevant cyber topics. Cybersafety is a 24/7, year-round commitment on the part of DoIT, and a key part of that is helping our community be informed and responsible. In the pages ahead, you'll find a focus on avoiding phishing scams, travel safety, relevant cybersecurity news, and information regarding updates to UMBC policies. We hope that these pieces will be able to play a role in helping everyone stay safe.

- **Stacy Cahill,** Chief Information Security Officer

TABLE OF CONTENTS

Welcome from the Chief Information Security Officer! **1**
Table of Contents **1**
Phishing Attacks **2**
UMBC Targeted: A Reminder of The Signs 2
Follow us on myUMBC! **5**
Travel Safety **6**
Information Security Abroad 6
News Bites **8**
Relevant news in cybersecurity 8
Concerns, threats, and things to know 8
Policy Updates **10**
UMBC Acceptable Use Policy 10
UMBC Information Technology Security Policy 10

Phishing Attacks

UMBC Targeted: A Reminder of The Signs

Phishing attacks are an unfortunately persistent issue, both in the campus community and the online world at large[1] [2]. These problematic schemes take numerous forms and employ tactics ranging from scare tactics to fake opportunities. They share a common goal: deceiving a victim into giving up their password or other sensitive information. Recent phishing attacks targeting UMBC have employed sophisticated methods, aiming to catch victims off guard with unique tricks.

Unearthing a potential scam is possible. If you remain calm, consider context, and take a look before falling into an attacker's trap, the odds are that you will be able to tell something is wrong. Knowing the signs can save you from significant trouble and help you keep your credentials, accounts, and identity secure. The following pieces are crucial in doing so.

[1] Report: Phishing Has Surged 400% Year-Over-Year
[2] AI and the Increasing Phishing Threat

Urgent Language

Receiving an urgent email can be quite distressing. For example, you could receive a notice that your account is shutting down. When that happens, it is human nature to panic when you are told something alarming. Scammers count on victims overlooking discrepancies and irregularities due to the panic induced by the immediacy of their messages. Instead of falling for this language, treat it as a sign of trouble, especially in conjunction with these additional characteristics.

Questionable Context and Legitimacy of the Sender

An out-of-the-blue email making an odd request is not normal and should never be followed through on. As urgent as the content sent may seem, and no matter how official the format appears, an unusual context or sender address cannot be ignored. Attackers impersonate trusted sources in part of their ruse to deceive a victim, hoping that inconsistencies and giveaways won't be noticed.

If possible, look up the sender's address. Does it match the source it is claiming to be? Sometimes, just a single character in the address has been changed, with the same going for links in the body of the email. Check the recipient list. Has this request been sent out to dozens of other people? Any discrepancy should raise an immediate alarm.

Keeping Credentials Safe

Prompts to enter your passwords and personal credentials into replies, online forms, or links are not normal; no credible organization or entity does this, including any UMBC administration department. Services like Google Forms are not for passwords. Social security numbers and financial information should be protected at all costs; unsolicited requests for this data are extremely irregular. No personal information should ever be given up in any way through an email at all; always double-check where you are entering your data.

The Importance of Professionalism

Everyone makes an occasional typo or spelling mistake, but an official email will not be poorly worded and filled with grammatical errors. While not always the case, many phishing emails can be detected through the presence of clumsy structure and out-of-touch wording. Additionally, they may also prompt you to take unusual steps to resolve an issue. This can include guiding you to an outside form in order to pay for a parking ticket or to open a document containing HR information instead of using an HR portal. Messages from official UMBC departments or figures will always be professional, succinct, and not deviate from standard procedure. When in doubt, always report phishing emails.

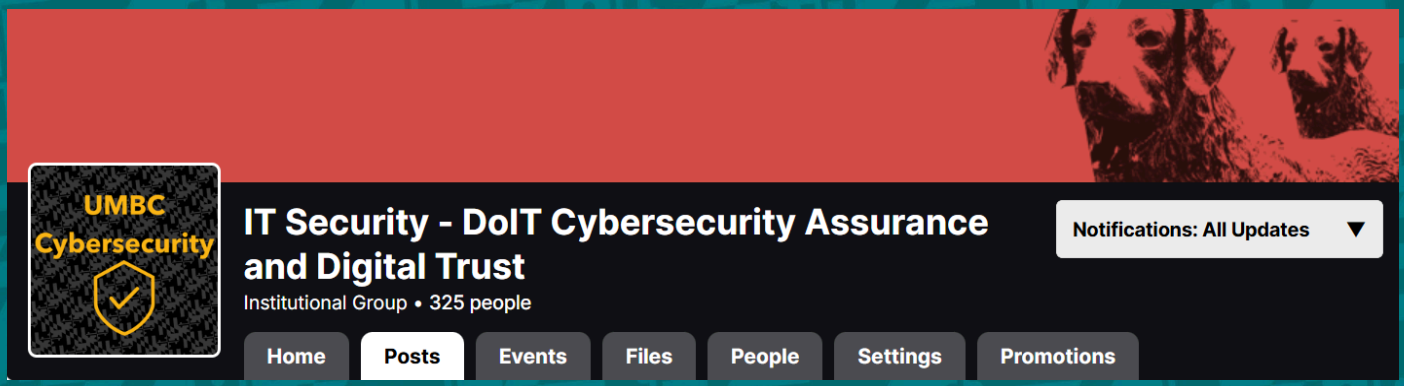
An Offer You *Can* Refuse

If something is too good to be true, it usually is. In juxtaposition to scare tactics and urgent wording seen in other common phishing tactics, attackers also lure victims through false, appealing opportunities. These include highly intriguing job offers, often for high pay and minimal effort, with the same goal in mind of extracting information. Always look up the company or individual and do the research to verify their existence. In the event of a scam, you will likely come back empty-handed, and not just in your search; if you aren't diligent, financial loss is very common in these situations.

Ignoring and Reporting

Regardless of the reason, whether you've directly spotted a sign or not, a potential phishing email should always be reported by forwarding the email to security@umbc.edu. In Gmail, the hamburger menu next to the sender contains a 'report phishing' button, also allowing you to directly report the message to Google. The email should never be interacted with in any way. Sometimes, something just feels 'off', and even that is enough. Stay alert to protect yourself.

The world is constantly changing, and attackers will always adapt. New traps and scams will continue to target both our campus and outside communities with relentless persistence. Despite this, we can always remain one step ahead by knowing the signs and practicing proper online safety. Being cautious and double-checking can go a very long way; it is an advantage that cybercriminals can never match.



FOLLOW US ON MYUMBC!

For regular updates about the most recent security alerts and phishing scams, follow us on my.umbc at https://my3.my.umbc.edu/groups/itsecurity

TRAVEL SAFETY

Information Security Abroad

You are more vulnerable to data breaches, unauthorized device access, identity theft, and additional forms of cybercrime when traveling[3] [4] [5] [6]. This means that information security is just as important as other elements of travel safety, and should not be overlooked when abroad. With a few simple precautions, you can take the initiative to keep your information, data, and devices secure, as outlined by DoIT's very own travel FAQ.

While risks vary depending on the destination, DoIT has several universal recommendations and items to be mindful of when traveling. Above all, exercise extreme caution when transmitting and possessing sensitive information. Your communications and activity can be intercepted, specifically on public WI-FI networks. Take proactive steps, such as installing recent updates and running active antivirus software, before you leave. No matter how safe the destination may seem, being mindful in this way is always the best practice. All travel circumstances are different, but these are the points that can and should be common practice no matter what.

[3] Travel Warning: Cybercrime Emerges As A Top Security Threat In 2025
[4] Mitigating the Risk of Cybercrime While Traveling Abroad
[5] Cyber Threats Remain a Top Business Concern in Travelers Risk Index
[6] Identity Theft Protection While Traveling

UMBC Email services can be used while abroad, but it is recommended to do so with safety practices in place, as is the case with Cloud Storage. There may be additional measures to take that depend on the country and its classification by the State Department. DoIT has specific guidelines and recommendations for each classification level regarding which devices to bring, alternatives, and the best data safety practices.

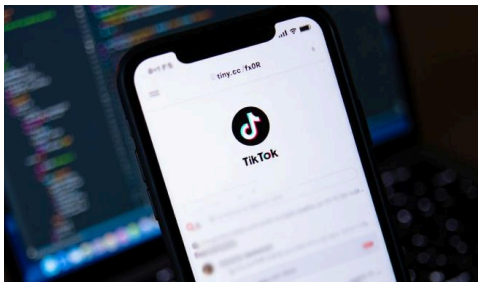
Whether you're traveling abroad for education, work, or simply vacation, the need for precautions remains the same. Even when you aren't in another country, there is a large amount of general advice that can and should be heeded in your day-to-day life. A safety-first mindset works, and the peace of mind it brings is invaluable. You should enjoy your trip and the experiences it brings, but be sure that those experiences don't include having your identity or research stolen.

For an in-depth rundown with extensive details on protecting information and devices when traveling abroad, please consult DoIT's Travel FAQ, dedicated to UMBC travelers and their safety onjourneys. It contains expanded information on all topics discussed above, as well as much more to help you stay informed and proactive.

NEWS BITES

Relevant news in cybersecurity. Concerns, threats, and things to know.

15,000 Fake TikTok Shop Domains Deliver Malware, Steal Crypto via AI-Driven Scam Campaign



Cybersecurity firm CTM360 has revealed an elaborate and widespread scam targeting TikTok Shop users. This campaign uses AI-generated TikTok videos and fake Meta ads to lure victims to more than 15,000 lookalike domains that impersonate TikTok's e-commerce platform. These sites either phish for credentials, trick users into downloading a trojanized app embedded with malware capable of harvesting sensitive data and crypto wallet details, or persuade people to donate cryptocurrency to fake storefronts or wallets under the guise of affiliate incentives.

FBI seizes domain storing bank credentials stolen from U.S. victims

The FBI and U.S. Justice Department recently seized the web3adspanels.org domain and its associated database. The database had been used by cybercriminals to store bank login credentials taken through phishing and account takeover attacks. The collection scheme saw U.S. victims tricked into visiting fake banking sites, resulting in millions of dollars in attempted and actual losses. This significant disruption of cybercriminal infrastructure was carried out with the help of international law enforcement partners.

QR Code Scams Surge as 'Quishing' Becomes a Mainstream Cyber Threat

QR Code Scams, also known as quishing, are becoming an increasingly major cybersecurity concern due to the ubiquity of QR codes and individuals' willingness to scan them. These scams see attackers use fake QR codes to trick people into visiting malicious websites or downloading harmful software. These codes are often placed in emails, public places, or even on fake delivery notices, making them hard to spot. Just like URLs, QR Codes should only be interacted with if coming from a trustworthy source.

Lost iPhone? Don't fall for phishing texts saying it was found

A currently active SMS phishing campaign is telling recipients that their iPhone has been "found" and is urging them to click on a link to recover it. The link leads to a fake Apple/iCloud login page designed to steal AppleID credentials and one-time codes. This scam can be avoided by not clicking on links in unexpected texts, and ensuring Find My- and iCloud are accessed only through Apple's official website or apps.

POLICY UPDATES

Last spring, DoIT revised four new policies. Complimenting long-standing values and commitments, these additions reaffirm standards for safety, responsibility, and professionalism. In addition to the following overviews of these changes, the official policy documents are linked for both viewing and downloading. Please consult the said documents for comprehensive details on each policy.

UMBC Acceptable Use Policy

UMBC provides a multitude of digital resources to support learning, research, and work. The usage of these resources carries both privilege and responsibilities, and any individual using them is expected to follow laws and licenses, respect the rights of others, use the resources for appropriate university-related activities, and act responsibly in their endeavors. UMBC may monitor and restrict access when needed in order to keep its systems secure. When you create an account, you agree to follow all rules in the broadest sense.

UMBC Information Technology Security Policy

This addition lays out the ways in which UMBC protects its information and technology systems. All data, networks, computers, and devices are important resources that need to be secured, including resources located both on campus and in the cloud. Everyone in the campus community, including students, faculty, staff, and contractors, has a role to play in protecting these assets. Key areas such as risk management, controlled data access, responsible use, emergency preparation, and incident response are vital in ensuring that data remains available and safe from misuse.

UMBC Policy on Credential Management, Authentication, and Authorization

In alignment with recognized standards for credentialing, authentication, and security, this addition pertains to UMBC's credential issuance management. It governs how UMBC generates and manages digital identities, how individuals authenticate their identities, and how access rights to systems and resources are granted and modified through processes such as risk-based controls. This policy addresses all UMBC community members, all of whom are issued a single primary credential. In addition to standard enforcement, DoIT is responsible for providing relevant guidance.

UMBC Policy on the Classification and Protection of Confidential Information

UMBC treats its data and information as valuable assets that must be safeguarded. Every member of the UMBC community is responsible for handling any confidential information appropriately, classifying it based on the level of risk, and protecting it from unauthorized access, use, or disclosure. There are four classification levels, and as the data becomes more sensitive, stronger precautions and safeguards apply. If any third party handles UMBC's confidential data, they must meet these same high standards of protection. Any data steward who suspects a leak or misuse of this data must immediately report it to the Chief Information Security Officer, who will begin taking appropriate action.

If you see something, say something!

Report all phishing emails to security@umbc.edu.

STAY SMART, STAY SAFE!

UMBC
AN HONORS UNIVERSITY