



RISKS | CONTROLS | COMPLIANCE ALERT

Volume 2 | Issue 1 | January – March 2021

“

Learn ways to be cybersecurity savvy.

”

IN THIS ISSUE

- [Maintain your vigilance against cybersecurity threats](#)
- [State of Florida Auditor General issues a clean report on FIU's financial position](#)

GETTING AHEAD OF THE CURVE

October is National Cybersecurity Awareness Month, and last year during that month, FIU's Division of Information Technology provided helpful tips to combat cyber attacks through a series of webinars it offered to staff and faculty. However, the threat does not end with the passage of October 31st. In fact, according to one source, *IT Governance*, in December 2020, they logged 134 security incidents accounting for 148,354,955 breached records, the highest number of publicly disclosed incidents they have recorded. *Security Magazine* reported that there were 2,935 publicly reported breaches in Q1 - Q3 of 2020 with some 8.3 billion records breached in Q3 alone. Cyber threat actors have attacked corporations of all sizes, governments at all levels, and educational institutions of all types—thus, the need for vigilance to protect against becoming a victim or an unknowing facilitator of cyber threat actors.

[Read more...](#)

[Back to the top](#)



RECENT SUCCESS

A recent audit of the Florida International University annual financial statements and its aggregate discretely presented component units for the fiscal year ended June 30, 2020, performed by the State of Florida Auditor General concluded that the financial

statements present fairly, in all material respects, the respective financial position of FIU and the discretely presented component units. Further, the Auditor General reported finding no material weaknesses in internal control over financial reporting or no instances of noncompliance or other matters that are required to be reported under *Government Auditing Standards*. These commendable results reflect the efforts of the University's Chief Financial Officer and the Office of the Controller.

You can find the full audit report at the following link:
[Florida International University Annual Report 2019-2020](#)

[Back to the top](#)

OTHER RESOURCES

- Need to report fraud, waste, and abuse? You may do so at: compliance.fiu.edu/hotline/ (hotline) or auditors@fiu.edu
- Need to report a Whistle-blower complaint? You must do so in writing to the OIA or call us at the contact information listed below.
- State University System of Florida Board of Governors' Regulations: flbog.edu

[Back to the top](#)

ABOUT US

The **FIU Office of Internal Audit** serves as an independent appraisal function for the University. Our audits of the University's colleges and departments evaluate financial processes, internal controls, and compliance with laws, rules, and regulations with a view towards ensuring that services are appropriately delivered in the most efficient and economic manner possible. Our Office is also responsible for conducting investigations for all allegations of fraud, waste, and abuse and whistleblower complaints.

Florida International University
Office of Internal Audit
11155 SW 17th Street, CSC 442
Miami, FL 33199

305-348-2107 | auditors@fiu.edu | oia.fiu.edu

TYPES OF ATTACKS AND WHAT TO DO

Phishing attacks

What it is:	Email, text, or phone communication that are crafted to lure individuals into clicking on a link or answering questions that will trick them into providing personal information, such as login credentials or credit card information, or downloading and installing malware.
--------------------	--

Phishing attacks can be delivered in several ways:

Deceptive Phishing	Attacks involve crafting and sending generic messages that arrive from seemingly legitimate companies or individuals to lure a user into verifying account and personal information.
	What to do
	✓ Hover over URLs to determine if they lead to suspicious or unknown sites
	✓ Check the FROM field for spelling errors or missing characters (e.g., "rory@microsoft.com" is displayed as "rory@microsoft.co")
	✓ Determine whether the tone of the message is forceful or unreasonably urgent
Spear Phishing	Attacks expand upon deceptive phishing by addressing a specific user by name, title, phone number, and other information to make the message appear more legitimate.
	What to do
	<ul style="list-style-type: none"> ✓ Take similar actions recommended for deceptive phishing ✓ Avoid publishing sensitive personal and corporate information on social media
Whaling	Attacks involve masquerading as senior-level staff to obtain sensitive information from other staff
	What to do
	✓ Use multi-step verification for sensitive internal and external requests (e.g., directly confirm the requests with the authentic sender)

Ransomware

What it is:	A form of malware that encrypts the files on a target system and renders the data inaccessible until a fee is paid to the attacker.
--------------------	---

Ransomware can be delivered in several ways:

Exploit Kits	Rely on exploiting weaknesses in the applications used to browse certain websites, such as your browser, Java, or Flash
	What to do
	✓ Ensure that applications are patched on a routine basis
Email Campaigns	Rely on crafting sophisticated phishing attacks capable of bypassing email filters to lure users into installing ransomware
	What to do
	✓ Follow the steps recommended in the phishing attack section above
Remote sessions	Untrusted sources or insecure applications can introduce ransomware to a system
	What to do
	✓ Use updated versions of FIU approved software, such as Microsoft Teams and Zoom
	✓ Only allow authorized users to join sessions

Social engineering	
What it is:	Attacks rely on psychologically manipulating people into disclosing personal information or performing actions. Attackers typically use social engineering tactics during natural disasters, epidemics, economic concerns, political elections, and holidays.
Social engineering attacks can be delivered in several ways:	
Emails	Sending phishing emails containing attachments and links to fictitious relief organizations to collect fraudulent donations or personal information
	What to do
	✓ Avoid opening attachments from unknown sources and exercise vigilance when making donations to unknown parties
	✓ Visit official sources such as the CDC and World Health Organization
Baiting	Sending emails for enticing users to purchase Personal Protective Equipment from fraudulent websites
	What to do
	✓ Never click on links from unknown senders
Pre-texting	Pretending to be insurance companies helping those potentially affected by COVID and attackers establishing fraudulent stimulus distribution websites
	What to do
	✓ Always contact a verified number prior to using the services of an unknown source