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")
	✓ Check for generic greetings
	✓ 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 to message appears more legitimate.
	What to do
	✓ 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
	✓ Require password to join sessions
	✓ 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