Cybersecurity Best Practices

This is a reminder to stay alert when reviewing emails, links, attachments, and online requests. Cyber scams and phishing attempts continue to increase, and attackers are becoming better at making messages look legitimate.

Please be especially cautious with messages that reference recent events, school systems, account issues, invoices, password resets, shared documents, or urgent requests. Threat actors may use publicly available information, or information obtained from recent third-party incidents such as the Instructure Canvas security incident, to make phishing emails appear more believable.

Please keep these best practices in mind:

- Don't click links or open attachments from unexpected or unfamiliar emails.
- Be cautious of messages that create urgency or ask for sensitive information.
- Double-check the sender's email address if something seems off.
- If a message seems unusual, verify it through a separate method, such as a phone call, Teams message, or a new email thread.
- Hover over links before clicking, and don't click if the destination looks suspicious.
- Never share your password, MFA code, verification code, or reset link with anyone.
- When in doubt, report it or contact IT/Security for guidance.

If you receive a suspicious email in your student email, please report it to IT Service Desk: 714-438-8111 or visit the Online Service Desk Portal.

Even legitimate-looking emails can be fake. Slowing down, verifying the request, and reporting suspicious messages helps protect our employees, students, and District systems.

Thank you for helping keep our workplace and information safe