The Faculty Member: One Quick Click Can Be Costly [1]

The

Even with the best intentions, mistakes can still happen—like clicking a suspicious link. What truly matters is how quickly and effectively you respond afterward.

What Went Wrong – The Setup

A faculty member received an urgent email that appeared to come from their dean, complete with familiar branding and a convincing tone. Pressed for time, they clicked a link to review a OneDrive document and entered their username and password, unaware that the page was a fake. Their username and password were stolen, giving attackers access to sensitive university systems.

The Cyber Safe Fix – Different Choices, Different Outcomes

- Pay close attention to communications that convey a sense of urgency or request prompt action [2].
- Hover over the link with your cursor to preview the domain. If it doesn't match the sender's organization or context, or if the visible link and preview differ, it's likely deceptive.
- Examine sender's address and look for slight misspellings or unusual domains.
- If a request is unexpected or urgent, verify it through another channel (e.g., Outlook email, phone call, Teams chat).
- Use Outlook's email security features to help filter future scams (e.g., report phishing button, block senders).

The Cyber Safe Recovery – What to Do After a Slip?up

- Reset your CU password immediately; if you reuse that password elsewhere, change those accounts, too.
- Immediately report the incident [3] to your campus IT service desk or information security. Quick reporting allows the investigative team to assess the impact and respond accordingly.
- Enable/confirm multi-factor authentication (MFA) [4] on your account to reduce the impact of stolen passwords.
- Monitor for unusual activity (outgoing emails, login alerts); notify your campus IT service desk or information security team if anything looks off.

More Real-Life Situations and Choices That Went Wrong

- The Administration Assistant [5]
- The Health Care Technician [6]
- The Department Manager [7]

About Information Security on Your Campus

Each campus employs an information security officer along with other security staff to safeguard data. They evaluate risks, implement security protocols, and address security incidents.

- CU Anschutz [8]
- CU Boulder [9]

- CU Denver [8]
- UCCS [10]
- System Administration [11]

Groups audience:
Office of Information Security
Right Sidebar:
Did You Know-Faculty Member

Source URL:https://www.cu.edu/security/faculty-member-one-quick-click-can-be-costly

Links
[1] https://www.cu.edu/security/faculty-member-one-quick-click-can-be-costly
[2] https://www.cu.edu/security/avoid-being-phishing-scam-victim [3] https://www.cu.edu/security/reporting-incident [4] https://www.cu.edu/security/multi-factor-authentication-added-protection-cybercrime
[5] https://www.cu.edu/security/administrative-assistant-when-password-reuse-opens-door
[6] https://www.cu.edu/security/health-care-technician-when-ignoring-updates-puts-your-device-risk
[7] https://www.cu.edu/security/department-director-mfa-fatigue-approving-wrong-request
[8] https://www.cuanschutz.edu/offices/information-security-and-it-compliance
[9] https://oit.colorado.edu/services/it-security [10] https://oit.uccs.edu/security [11] https://www.cu.edu/uis