From the University of New Hampshire- Signs your Email Account is compromised…

Inbox Rules You Didn't Create - If a co-worker or family member asks about an email they sent that you don't remember getting, check to see if there are any inbox rules set-up to automatically forward/move/delete emails. A common tactic used by cybercriminals is to immediately set-up rules to divert or re-route emails when they arrive in your inbox. This allows them to use your account without you noticing.

Emails in Sent Folder You Didn't Send - If a cybercriminal uses your account to send spam or phishing emails, you may see evidence of those emails in your Sent Mail folder.

No Emails in Your Sent Folder - In some cases, cybercriminals will delete all the email in the Sent Mail folder in an attempt to hide/cover their tracks.

Inability to Log In to Your Accounts – In some cases, the first action an attacker takes once they get access to your account is to change the password. In other cases, UNH IT may have secured you due to a suspected or confirmed compromise.

Last Logged in Date/Time Stamp that Doesn't Make Sense – If you are using a system that provides you with the last date and time you logged in to that application and that date and time stamp doesn't align with the last time you believe you accessed the account, it can indicate someone else has been accessing your account.

Confirmation Emails Received for Actions You Didn't Take – Receiving email confirmations for things like password changes on other accounts, online purchases, and online newsletter subscriptions that correspond to actions that you did not take is a good sign that someone else has access to one or more of your accounts.

Reports from Others of Email Received from You that You Didn't Send – If co-workers, family members, or others tell you they received email you didn't send or respond to email you didn't sent, your account is compromised.