ITS Communications

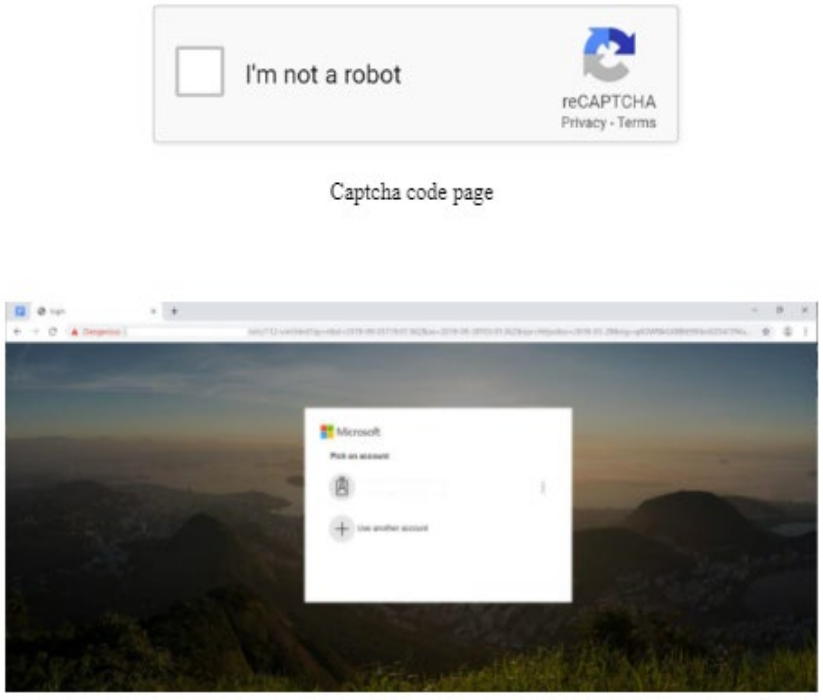
Algonquin College
Cybersecurity Awareness Month
2024

Phishing & Captcha Codes

Be on the lookout for a new phishing campaign that uses Captcha codes.

After clicking a link in the email, the recipient is redirected to a page that contains a Captcha code. The Captcha code site does not contain any malicious items, enabling the email to make it through technical controls. After completing verification, the recipient is redirected to the real phishing page that contains a fake login page designed to steal credentials. If the recipient enters login information, it is captured by the attackers.

SEE AN EXAMPLE OF THIS THREAT BELOW



Captcha code page

Fake login page

1. **Scrutinize all email requests.** Be on the lookout for popular phishing narratives like shared documents, overdue payments, order requests, and invoices.
2. **Remember, phishing emails consistently make it past technical controls.** Attackers are constantly evolving their techniques and disguise malicious links by using Captcha code pages or QR codes.
3. **Always verify.** Phishing emails often use brands and images you recognize to create a sense of trust. Call the sender to verify the email is legitimate if anything looks unusual.

Remember, you are the last line of defense against phishing.
IF YOU RECEIVE A SUSPICIOUS EMAIL, REPORT IT IMMEDIATELY.

Report Phishing

Information Security & Privacy is Everybody's Business