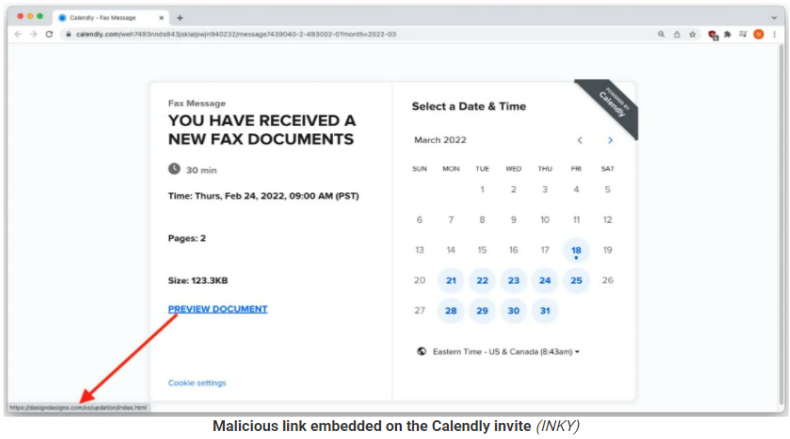
eHealth Saskatchewan

Enterprise Security Services

Popular Brands Used In Phishing Emails To Steal Credentials



Malicious link embedded on the Calendly invite *(INKY)*

Cybercriminals regularly spoof well-known brands to harvest credentials for later cybercrimes.

Emails generated and sent by legitimate platforms (ie. Microsoft, Google) are commonly considered trustworthy by email security tools, so they tend to reach targeted inboxes rather than the spam folder.

Spoofing popular platforms to distribute malicious links blends very well with the daily work background of most victims, so it's unlikely these attempts would raise suspicions.

The use of brand logos and trademarks adds visual trickery leading to the successful impersonation of well-known brands, like free calendar app Calendly.

Think Twice!

Cybercriminals often distribute malware using email attachments or by tricking users to click links directed to malicious internet content.

Be the strong link!

- ☑ Never click on links and buttons in unexpected or suspicious emails or text messages. This is how ransomware is delivered.
- ☑ Only use approved software and applications. Make sure to only install from a trusted source.
- ☑ Never modify or disable antivirus software installed on your computer. It only protects you if it is enabled and updated!
- ☑ Examine the sender's email address and display name carefully. Also, hovering over a link will reveal its true destination.

If you suspect you've received a suspicious email, forward it (as an attachment) to emailsecurity@eHealthSask.ca and delete it from your inbox. Report any security-related incidents immediately to ServiceDesk@eHealthSask.ca

We appreciate your help in protecting the Saskatchewan health network.