Published on *The National Law Review* https://natlawreview.com

Privacy Tip #349 – College Students Targeted by Social Engineering Campaign Impersonating Instagram

Article By:

Linn F. Freedman

Dark Reading reports that thousands of college and university students are being targeted by cyber-attackers who are using a legitimate domain to impersonate Instagram and steal credentials of the users. The attack is able to evade security measures of Microsoft 365 and Exchange.

According to the report, "The socially engineered attack, which has targeted nearly 22,000 mailboxes, used the personalized handles of Instagram users in messages informing would-be victims that there was an 'unusual login' on their account." The attackers also sent email messages to the victims from a valid email domain, which made it more difficult for users and security technology to identify it as malicious.

The email impersonating Instagram uses a familiar tactic to lure victims into believing it to be true: a sense of urgency. The email appears to come from Instagram's support team and includes the sender's name, Instagram profile, and email address. The user is then informed that "an unrecognized device from a specific location and machine…had logged in to their account," and asked to click on a link asking them to "secure" their login details, which of course redirects the user to a fraudulent landing page that then allows the attackers to steal the user's credentials.

The researchers from Armorblox who investigated the scam suggest that users watch out for social engineering cues, review all emails for any inconsistencies, and employ multifactor authentication and password-management best practices across both personal and professional accounts.

National Law Review, Volumess XII, Number 327