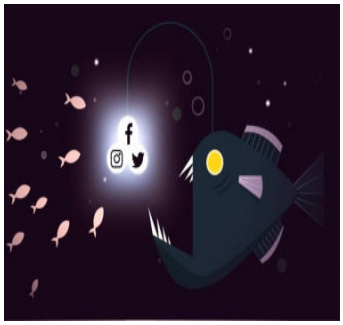
Volume 3 Issue 1 Date: 01.04.2026

Cybersecurity Digest

Bi-Weekly Update by the O/o CISO of Meghalaya Rural Bank

MEGHALAYA RURAL BANK

Angler Phishing



Phishing remains a leading cyber threat in 2025, responsible for a vast number of data breaches. Phishers now exploit newer channels beyond email – including social media – to trick victims.

Social platforms like Twitter/X, Facebook and Instagram are home to an emerging phishing scheme called **angler phishing**.

In an angler phishing attack, the criminal impersonates a company's customer service account on social media and lures unsuspecting users into scams. By hijacking brand identities and replying to public complaints or queries, angler phishers trick people into revealing credentials or clicking malicious links.

Angler phishing is a social media-based phishing attack in which scammers pose as customer support agents. The attacker creates a fake profile (often using a company's name, logo, and branding) on a platform like Twitter/X, Facebook or Instagram.

When a real customer publicly complains or asks for help, the phisher "fishes" by responding from the bogus account. They present themselves as helpful support, but their real goal is credential theft or malware delivery.

How Angler Phishers Manipulate Social Trust

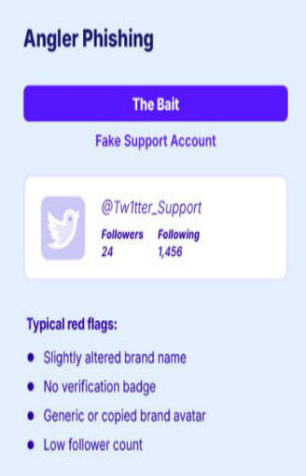
Angler phishers exploit the trust people have in official support channels. They often **monitor social feeds** for frustrated customers. For example, when someone tweets: "my online order never arrived," the attacker swoops in pretending to be the brand's support team.

The fake response might say: "We're sorry for the trouble! Please click here so we can verify your account and fix the issue."

The link leads to a malicious site or download. If the user clicks, the site may install malware or prompt for login details. The attacker then harvests this sensitive data to hijack accounts or commit fraud.

Key tactics in angler phishing include:

- **Impersonation of Official Accounts:** Attackers create accounts with names and avatars mimicking legitimate support channels. They may add words like "support," "help," or slight misspellings (e.g. "@Facebokhelp" instead of "@FacebookHelp").
- **Targeting Public Complaints:** They focus on users who are already upset or looking for help. Angry or worried customers are more likely to trust a quick reply.
- **Malicious Links and Requests:** The fake support message typically includes a link or asks for account details. Clicking the link may download malware or open a spoofed login page. Victims might be asked to *"confirm"* their password or enter a security code – which the attacker then uses to take over accounts.



Unlike email phishing, these scams appear in public or direct messages where people assume official help is nearby. The attacks are insidious and persuasive: victims may genuinely think they're getting help, when in fact they're giving attackers the keys to their accounts

A Realistic Angler Phishing Scenario: How It Unfolds

A typical angler phishing incident might play out like this: Jane posts on Twitter that her internet service has been unexpectedly cut off. Within minutes, a message appears from a handle like **@FastNetSupport** (note the company name spelled correctly, but the account is newly created).
The message says: "Sorry about your connection issue! Click here to verify your account." The link points to a web page that looks like the internet provider's login portal. Jane, grateful for quick help, enters her username and password.
Unbeknownst to her, this is a trap: the fake site captures her credentials, giving the attacker full access to her account. Meanwhile, Jane thinks the issue is resolved – until her account is drained or hijacked.
This scenario illustrates how angler phishing works: by masquerading as official support and leveraging urgency, attackers **dupe users into trusting malicious links and divulging sensitive information**.

Recognize and Block Angler Phishing Attempts

Defending against angler phishing requires both technology and awareness. Organizations should educate users and enforce security measures:
1. Verify Official Accounts
Always double-check that social media responses are from legitimate company profiles. Look for verified badges or compare URLs and usernames carefully before interacting. If in doubt, initiate a new support request via the company's official website or known channels.
2. Be Cautious with Links and Attachments
Never click links or open attachments from unsolicited social media messages. Instead of clicking, independently navigate to the official website or support portal. Hover over links (if possible) to see the actual URL and ensure it matches the real domain.
3. Use Multi-Factor Authentication (MFA)
Require MFA for all important accounts. Even if credentials are phished, MFA can prevent attackers from using stolen passwords alone to log in. (Phishing-resistant methods like hardware tokens or authenticator apps provide stronger protection than SMS codes.)
4. Block and Report Fake Accounts
When users spot suspicious support accounts, they should block and report them immediately to the social platform. Reporting helps the platform take down malicious profiles and protect other users.
5. Train with the SLAM Method
Incorporate phishing awareness training focused on social media threats. For example, the SLAM method teaches users to examine the *Sender*, *Links*, *Attachments* and *Message* of any communication for red flags.

The Bottom Line

Angler phishing capitalizes on the fact that customers who are in need of support may be quick to comply with the requests of a scammer who they believe is offering genuine help. Phishing is a constant threat, but your best defense is to simply hit pause, listen to your gut and avoid making any decisions in the heat of the moment.
Take time to consider any requests for action on your part. When in doubt, simply disengage. Then, reach back out to the organization using a trusted form of communication, such as a phone number or live chat support found directly on the organization's official website.
Beyond angler phishing, stay aware of other common phishing scams to help avoid falling into traps