



Don't Take the Phisher's Bait

Everyone receives a lot of emails every day. "Sign up for this," or "Become a member of that." We often don't give those emails a second thought. But, when you get an invoice or important update from a company you think is one you trust, it may be difficult to know whether or not it is a scam.

Scammers posing as reputable companies send faux invoices to users for items and services the user did not purchase. For example, a scammer posing as a computer support representative of a reputable company may call you or send a phishing email. It only takes one time for you or someone at your place of work to be convinced that the "trusted company" needs to install a program or needs access to your computer for "patch management" purposes and your system will become compromised. Again, if you assume the scammer is a legitimate representative and you allow access to your private home computer or a computer on your employer's network, the entire system could be at risk.

Following are a few tips to help avoid taking the phishing scam bait:

- Verify the facts – If the company doesn't sound familiar, or if you don't remember making a purchase, do not open the attachment or click on the link. Review your purchase records first.
- Call them back – If a supposed company calls for access to install patches for information that sounds suspicious, ask for their name, hang up, and call the company back from a number you already have for them and ask for the person who called you. Do not call back the number that they called you from.
- Slow down – Phishing schemes and scammers may try to pressure you by saying the issue is time sensitive. Always take time to double check if you sense a red flag. Fact checking will save you a lot of time, and money. Don't put yourself or your employer/company at additional risk.

Cyberattacks, such as phishing attacks or social engineering, are becoming increasingly common. North Central Bank is committed to helping you manage and mitigate cyber risks. Please reach out to one of our helpful staff members for additional tips on how to reduce your chances of being scammed.

126 E High Street
Hennepin, IL
815-925-7373

110 N Main Ave
Ladd, IL
815-894-2386

Member FDIC

Additional credit to BankOnIT, 8601 Commerce Park Drive, Oklahoma City, OK 73132
for suggestions and information regarding phishing