

WATCH OUT FOR TELEPHONE SUPPORT SCAMS



Recently an unknown telephone caller purportedly from “Microsoft” attempted to convince a UNL employee to allow him to remotely connect to the employee’s computer to “check out his computer”. The security conscious employee did not fall for this scam and notified the UNL ITS Security Team.

This is a new version of an old scam where cybercriminals call you and offer to help you solve computer problems or sell you a software license. Cybercriminals often use publicly available information to gain your trust, and might even be able to guess what operating system you are using.

Once they've gained your trust, they may:

- Ask for your username and password.
- Ask you to install software that will let them access your computer to fix it.
- Ask for credit card information.

To protect yourself from telephone tech support scams:

- Do not purchase software or services over the telephone, especially from a stranger.
- Never give control of your computer to a third party unless you can confirm that it is a legitimate representative of a support team with whom you are already a customer.
- Take the caller's information down and immediately report it to your local authorities.

UNK Information Technology Services may call you if we discover a malware-infected computer. These calls will go through your Technology Coordinator or come from our Helpdesk. If you are ever concerned about the legitimacy of a support call, hang up and call the UNK Helpdesk at (308)865-8363.