IT Security – New Phishing Attempts Using Remote Monitoring and Management Software (RMM)

All associates are responsible for maintaining awareness of possible phishing attempts coming to their company email and reporting any suspicious emails.

The Cybersecurity & Infrastructure Agency (CISA) recently released a warning about a new phishing scheme using remote access software. Attackers send an email posing as a legitimate company, most often these emails look like help-desk emails and contain phone numbers to call or links to a malicious site. From there the attacker would download legitimate RMM software to gain complete access to the victim's computer. These victims are then tricked into logging into their bank account and the attacker would modify the screen to show a large amount of money in the account that was accidentally "refunded." The victim is then convinced to send this money to the attacker.

Some tips to recognize these emails and prevent becoming a victim:

1. If you are not expecting an email from that company, it is likely not legitimate
2. When in doubt, check on the company's site for a legitimate phone number to check and do not call the phone number given as it may be compromised
3. Do not click any links coming from a suspicious external source
4. Remember to never give anyone access to your computer other than the company IT team.

If there are any doubts about an email contact IT.

For more information about this you can visit
https://www.cisa.gov/uscert/ncas/alerts/aa23-025a