AtNetPlus

(330) 945-5685 | atnetplus.com

SCAMMERS ARE WREAKING HAVOC WITH JUST A CELL NUMBER

With this new phishing threat, scammers are sending out an email impersonating the owner of a company, the Human Resources Department, or a manager. Usually, these emails are simply a short request asking for a cell phone number to “update” the contact list or expressing the need to immediately contact the targeted employee.

What happens after a scammer knows your cell phone number?

Once a scammer gets a name and cell number, they will often continue to attempt to gather as much additional Personal Identifiable Information (PII) as possible including address, social security number, date of birth, or any other information that can be used for identity theft. Then, they contact the mobile provider *(impersonating the victim)* to inform them that the phone was stolen and request the number be “ported/transferred” to another provider and device. In some cases, they visit a retail location to try to buy a new phone taking a chance that a sales representative who’s incentivized to quickly fulfill their request will forgo the formal verification procedures.

This typically begins a race where the scammer, by receiving the victim’s private texts and calls, tries to reset the access credentials for as many of the victim’s financial and social media accounts as possible before the victim realizes they have lost service on their device. Once the scammer has access, they attempt to drain any connected bank accounts or even attempt to sell access back to the victim *(like ransomware).*

HOW TO PROTECT YOURSELF

1) **Set up a Pin/Passcode with your cell phone provider.** This will act as a form of Multifactor Authentication. This helps verify that the user is the actual owner of the number preventing unwanted access to the account by outside parties.
2) **Inquire with your wireless provider about port-out authorization.** Every major wireless has additional security layers which make it more difficult for someone to port-out your phone number. Contact your mobile provider and speak to them specifically about porting and/or security on your account.
3) **Watch out for unexpected “Emergency Calls Only” status.** Contact your mobile phone company if your phone suddenly switches to "emergency call service only" or something similar. That is what happens when your phone number has been transferred to another phone.
4) **Be vigilant and aware of the communications you receive.** Watch out for phishing attempts, suspicious alert messages from financial institutions, or unexpected texts requesting a login code.