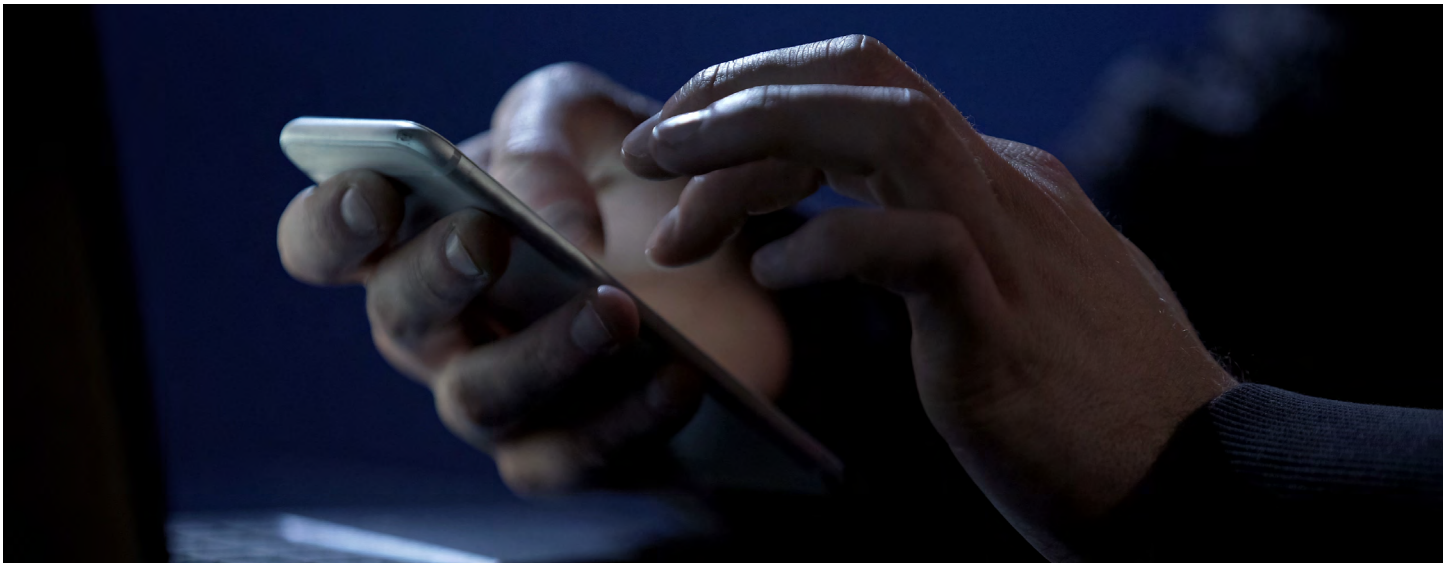
What Are Port-Out Scams?



When you think of cybercrime, you probably never think of it taking place through your cell phone. However, your phone is a significant point of vulnerability that criminals can exploit. Through something known as a port-out scam or an unauthorized mobile phone porting, cybercriminals can not only view your call and message history but can use your phone to gain access to your most sensitive data.

Here's how it works. If a cybercriminal gets a hold of your cell phone number, they will call your service provider and ask for the phone number to be ported over to a different SIM card, usually on a burner phone. To do this, they will have to provide whatever personally identifiable information your provider may ask for to process the request, such as your address, birthdate, social security number, etc. In an alternative method, they can go to one of your cell providers retail locations with a fake identity claiming to be you. They will then buy a phone and have your number ported to it. Once they have your cell phone number ported to their phone, they can use it to gain access to any service where your cell phone is a possible password recovery tool.

> *Certain laws mandate that cell providers must make it easy for customers to switch their number to a new provider, as long as they can verify their identity.*

If you've ever opted to do two-step verification by having a code texted to your cell phone, imagine that those codes instead went to a cybercriminal, and that's how it works. If a criminal has your login for your online banking, for instance, they can use the "forgot password" steps, and opt to have the verification code sent to "*your*" cell phone. After that, they can reset your password and gain online access to your bank account. Often, once they have access to your cell phone number, they can use it to get

inside your work email or text your contacts as part of a social engineering scheme. They could text your friends or parents asking to borrow money claiming it's an emergency.

When your phone is ported, you will notice that you no longer have cell service. After that, you'll probably see that access to services like bank accounts are denied since your passwords will have been changed.

Porting scams can become quite elaborate, and a friend at another company came very close to being the victim of one. The criminal first got control of his email and sent his CFO a request to wire $3,000 to a specified bank account. The CFO called his bank to process the wire without question. His bank, following standard procedure, called him to confirm the wire, and the hacker, having ported his phone, answered and confirmed that the wire needed to be processed immediately. Luckily the bank employee, who knew the customer's transaction history, found this suspicious and called the secondary number (the customer's wife) to double check, thus revealing the scam. If the employee had not been diligent and followed his instincts, $3,000 could have been lost.

What Can You Do?

Call your cell provider and ask how you can add additional security to your account. Most cell providers will allow you to set up a secondary password which will be needed to port your cell phone number or make other significant changes. If you have one of the four major carriers, click one of the links below to learn how to do this.

- Verizon
- Sprint
- T-Mobile
- AT&T

In general, be cautious about who you give your cell number to. When signing up for new services or websites, never provide your number unless you absolutely have to. Try and keep your email inbox clean of old phone bills or other items that could reveal your number. Lastly, make sure to change your passwords every couple of months, and don't make it anything potentially easy to guess.

If you ever suspect that your phone has been ported, call our customer service line at 800-330-9890 as soon as possible.