CYBERSECURITY AND DATA PRIVACY

THE NUMBERS DO LIE: HOW THIEVES CAN STEAL YOUR CELL PHONE NUMBER AND WREAK HAVOC ON YOUR LIFE

by Justin L. Root, Sara H. Jodka and Wendy G. Hulton

If you have an online account, you are familiar with the username/password method of user authentication. If you have been paying attention to recent news stories, however, you also recognize that this method of authentication has some security drawbacks. A quick visit to the website www.haveibeenpwned.com can help identify if your email address has been involved in a security breach, such as the breach that occurred at LinkedIn in 2012. In that breach, user email address and site passwords (stored as SHA1 hashes without salt) were stolen, and many were cracked to reveal the true text of the user's password. This meant that users who re-use passwords across platforms were susceptible to having other accounts accessed by the password thieves (or those to whom the thieves sold that information).

As both a remedial and preventative measure, users can employ the use of a password manager or, preferably, can enable a form of multi-factor authentication ("MFA," sometimes referred to as "2-factor authentication" or "2-step verification") to prevent stolen credentials from being used to access other accounts. One form of MFA used commonly is to have the service provider send a message with a one-time code to a trusted device, such as a cellular telephone, during a log-on attempt. Users of Apple's iCloud, Google's Gmail, or Microsoft's Xbox who have enabled MFA may already be familiar with this process. And it can be used on a variety of platforms, from social media to online banking. But what if someone stole not your cell phone, but your cell phone number and therefore received your calls, text messages, and MFA verification codes? In an emerging fraud trend, criminals are doing just that. Fortunately, there is a way to protect yourself.

This week, T-Mobile began notifying its users of a "port-out scam" affecting all of the cellular telephone industry. In a port-out scam, fraudsters impersonate legitimate users to transfer service for a cellular telephone number to a device in the fraudster's possession. That person would then begin to receive messages meant for the victim, which could include MFA codes, banking information, personal communications, or other sensitive and confidential messages or media.

Targeting a specific individual to facilitate fraud is not new. Spear-phishing emails have existed for years, through which fraudsters target specific people in a company to attempt to defraud the company. W-2 scams try to convince company workers to send all employees' W-2 information to fraudsters. CEO scams target a company's finance department to attempt to facilitate wire transfers. General phishing messages may try to obtain various employees' log-on credentials. It is not a far jump to identify a person's cellular telephone number and add that to the various schemes by which criminals can facilitate fraud, especially if your cellular telephone number is published or otherwise known widely. Indeed, receiving a telephone call or text message from a company contact—and being able to respond to that call or message at the correct cellular telephone number—would add a lot of credibility to a fraud scheme.

Fortunately, you can protect yourself (and your company) against port-out scams. Simply contact your carrier's customer service department and inquire about adding a security code to your account. Once added, changes can be made to an account only if the person requesting the change knows the code. It is therefore important that the code be kept confidential and secure. If you are not sure whether you and your company are protected against port-out scams or other forms of digital or electronic fraud, contact the Dickinson Wright Data Privacy and Cybersecurity attorneys to review your security policies, protocols, and training programs today.

FOR MORE INFORMATION CONTACT:

Justin L. Root is Of Counsel in Dickinson Wright's Columbus office. He can be reached at 614.591.5465 or jroot@dickinsonwright.com.

Sara H. Jodka is Of Counsel in Dickinson Wright's Columbus office. She can be reached at 614.744.2943 or sjodka@dickinsonwright.com.

Wendy G. Hulton is a Partner in Dickinson Wright's Toronto office. She can be reached at 416.777.4035 or whulton@dickinsonwright.com.