Shields Up/HaveIBeenPwned

What I Did

First, I tested the most common and troublesome internet ports by using the Internet Common Ports Probe on Shields Up. The probe sent a request to 26 different ports: 0, 21, 22, 23, 25, 79, 80, 110, 113, 119, 135, 139, 143, 389, 443, 445, 1002, 1024, 1025, 1026, 1027, 1028, 1029, 1030, 1720, and 5000. Each request could return no response, closed port or open port, which corresponds to a status of stealth, closed, or open. Second, I tested my system's first 1056 ports, using Shields Up's Internet service ports "grid scan." The grid scan works similarly to the Internet Common Ports Probe but checks ports 0 through 1055. Third, I used HaveIBeenPwned to check if two of my emails or phone number had been compromised in a data breach. HaveIBeenPwned currently checks email addresses and phone numbers against a database of 12,442,563,611 accounts that have been compromised in data breaches. Then, I used HaveIBeenPwned to check four different passwords that I commonly use. HaveIBeenPwned currently checks passwords against a database of hundreds of millions of passwords that have been exposed in data breaches.

What Are My Results

When I ran the Internet Common Ports Probe on Shields Up, my system failed because of a Ping Reply. A ping request was sent to the system, and my system replied, which makes it visible on the Internet. To fix this issue, I can further research how to configure my personal firewall to block, drop, and ignore ping requests. Fortunately, the status of each port tested was stealth, so none of the other requests received a response. When I tested my system's first 1056 ports, using Shields Up's Internet service ports "grid scan," the same issue occurred. My system failed because of a Ping Reply, but the status of ports 0 through 1055 was stealth. When I used HaveIBeenPwned to check two of my emails and phone number, both of my email addresses failed. One had been compromised through data breaches of Chegg and ParkMobile. The other email had been compromised through data breaches of Chegg and Avvo. To fix this vulnerability, I could create a new email. Fortunately, my phone number passed and had not been compromised in a data breach. Then, when I used HaveIBeenPwned to check four of my passwords, they all passed. None of them had been exposed in a data breach.

What Did I Learn

From this exercise, I learned that it can be very easy at times for hackers to obtain information that we would not want them to have. Fortunately, my system, phone number, and passwords appear to be pretty secure. I will fix the ping reply issue on my system. Then, it should pass the Internet Common Ports Probe and Internet service ports grid scan on Shields Up. I was surprised that the ports tested all came back green, but I'm very happy about it. For my email address, I had already been thinking about creating a new one. So, I may do that soon, since each email address that I commonly use was compromised in two data breaches. I will definitely use Shields Up and HaveIBeenPwned in the future to make sure my system, email address(es), phone number(s), and passwords are not vulnerable. Also, I will recommend both websites to others, so they can test their systems, email addresses, phone numbers, and passwords and protect themselves, too.