| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Z | Y | X | W | V | U | T | S | R | Q | P | O | N | M | L |

| P | Q | R | S | T | U | V | W | X | Y | Z | ! | @ | . | , |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| K | J | I | H | G | F | E | D | C | B | A | @ | ! | , | . |

R OLEV XIBKGLTIZKSB@

I LOVE CRYPTOGRAPHY!

T-Mobile had a major security breach just last year where data containing the social security numbers, names, addresses and driver's license information for more than 100 million people was leaked. The 21 year old hacker, on reddit, gave this explanation for the data breach

"The breach was done to retaliate against the US for the kidnapping and torture of John Erin Binns (CIA Raven-1) in Germany by CIA and Turkish intelligence agents in 2019," the hacker allegedly told Gal. "We did it to harm US infrastructure."

He said he gained access to the T-moible servers through "production, staging, and development servers two weeks ago." I'm not entirely sure what this is. But it looks like since then T-mobile has been stepping up its cyber security to make sure something like this won't be happening again. To improve cybersecurity moving forward, T-Mobile entered into a long-term partnership with Mandiant and consulting firm KPMG.