## 2016 Presidential Campaign Hacking Fast Facts

The 2016 presidential campaign type of attack was phishing which uses email, SMS, social media, phone, etc. to obtain a person's personal information. This vulnerability was discovered because the FBI contacted the Democratic National Committee’s help desk by letting the IT department know that one of their computers has been compromised by Russian hackers (September 2015). Which led to John Podesta receiving a phishing email that made him believe that someone tried to access his Google account, so he followed instructions to change his password which allowed the hacker to have access to his information. The hacker took advantage of the vulnerability because Podesta was not able to determine or have knowledge that it was a phishing email which allowed the hacker to dig into his information and it allowed them to send mass phishing emails to other people that were part of Hilary Clinton’s campaign because they had access to Podesta’s email release cell phone number and personal email addresses, publish stolen documents, and so much more. There could have been various measures that should have been taken considering this is a presidential election by education their staff so they understand basic of cybersecurity, staff should report to the IT department if they received email similar to wordings where people have accessed their account or for anything that have linked provided or they are unsure of to confirm, stopped using the hacked computer until they were able to find the source of attack, and there should had been stronger security services, IT should of had something that covered emails that were sent to campaign account under reliable @\_\_\_\_.com, overall campaigns should be more aware of these thing during election time because as it is a battle for presidency campaign people feel passionate about who their president should be.

## Hackers Claim They Breached T-Mobile More Than 100 Times in 2022

The T-Mobile attack in 2022 was phishing. The vulnerability was discovered through Telegram chat logs by three different cybersecurity groups because they conducted their business through open channels on the instant messaging platform and the author did not want to reveal the groups to prevent the cyberattackers to move their services on a more private platform. The attackers were able to take advantage of the victims because they did not know that they were being attacked or they did not understand or gather the concept of what was going on. Based on the article, these attackers would call the employee’s on their mobile devices, pretend to be someone from the company’s IT department, and try to get the person on the other end of the line to visit a phishing website that mimics the company’s employee login page. This allowed the attacker to take advantage of the fact that they have access to customer’s personal information such as: access to any financial, email, and social media that were tied to their phone number. They also ripped off the customer that they were able to phish to make them believe that they have access to services that they didn’t. Security measures that could have been taken to prevent this attack is that the company should of had two factor authentication on both the victim’s end as well as the corporate’s end this would improve overall security because if the attackers tried something similar again they the victim would be able to know whether is it an attack or not because soon afterward when hitting the login button it will take you to a page that required you to do two factor authentication. Since the employees were the target if ‘tickets’ were submitted for IT Support it should either be handled within the same day, or there should be logs that are dated with the case number to prevent this.