Group 6

W05 Case Project: Propose Your Project

Bradford Hogge

Capital One was hit by a massive security breach in July of 2019. In this breach, the hacker gained access to over 100 million accounts. This was done through a configuration vulnerability in a web application firewall. The hacker was able to gain access to customers’ personal information, such as names, addresses, phone numbers, birthdays, emails and self-reported income. About 140,000 social security numbers were also compromised because of the vulnerability. Capital One is a nation-wide credit union, yet they let something as crucial as social security numbers slip into the hand of someone unauthorized. We must study this situation more so that we don’t run into a similar security downfall like Capital One had.

Matthews, Kayla. “Incident Of The Week: Historic Capital One Hack Reaches 100 Million Customers Affected By Breach.” *Cyber Security Hub*, Cyber Security Hub, 2 Aug. 2019, www.cshub.com/attacks/articles/incident-of-the-week-historic-capital-one-hack-reaches-100-million-customers-affected-by-breach.

Kyle Tolliver

Windows had a security breach in January, which all started with a Zero day on Internet Explorer. This breach lasted since December 5 of 2019. Millions of users passwords and personal information was exposed online. The US Government issued the windows critical update. It is not very common for the government to issue a critical so this is very important.

Winder, Davey. “Microsoft Security Shocker As 250 Million Customer Records Exposed Online.” *Forbes*, Forbes Magazine, 23 Jan. 2020, [www.forbes.com/sites/daveywinder/2020/01/22/microsoft-security-shocker-as-250-million-customer-records-exposed-online/#38096ed64d1b](http://www.forbes.com/sites/daveywinder/2020/01/22/microsoft-security-shocker-as-250-million-customer-records-exposed-online/#38096ed64d1b).

“CISA Releases Emergency Directive and Activity Alert on Critical Microsoft Vulnerabilities.” *CISA Releases Emergency Directive and Activity Alert on Critical Microsoft Vulnerabilities | CISA*, www.us-cert.gov/ncas/current-activity/2020/01/14/cisa-releases-emergency-directive-and-activity-alert-critical.

“Alert (AA20-014A).” *Critical Vulnerabilities in Microsoft Windows Operating Systems | CISA*, www.us-cert.gov/ncas/alerts/aa20-014a.

McKayla Plummer

Sprint was hacked, again, through Samsung’s website. There were two big data breaches in 2019 for them. This second attack happened by credential stuffing Samsung.com’s “add a line”.

<https://www.zdnet.com/article/sprint-says-hackers-breached-customer-accounts-via-samsung-website/>

<https://www.zdnet.com/article/sprint-says-hackers-breached-customer-accounts-via-samsung-website/>

<https://www.cnet.com/news/sprint-customer-accounts-breached-by-hackers/>

<https://www.cpomagazine.com/cyber-security/sprint-data-breach-exposes-customers-to-unknown-attackers-will-this-impact-the-t-mobile-merger/>

<https://www.securitymagazine.com/articles/90560-sprint-confirms-data-breach-for-second-time-in-2019>

Eduardo Urbiola

Users of the newly released Disney+ streaming services were locked out of their accounts after being hijacked by fraudsters.

Disney+ members’ login credentials, including usernames and passwords. The BBC claims to have found several hacked customer accounts for sale on the dark web for as little as $3.

Forbes, *“Thousands Say Their Disney+ Accounts Were Hacked; Here’s How To Protect Yourself”*  [Dana Feldman](https://www.forbes.com/sites/danafeldman/) Senior Contributor [Hollywood Entertainment](https://www.forbes.com/hollywood-entertainment)

<https://www.forbes.com/sites/danafeldman/2019/11/19/thousands-say-their-disney-accounts-were-hacked-heres-a-way-to-check/#5199246b13bc>