Kyle Tolliever

McKayla Plummer

Bradford Hogge

Eduardo Urbiola

Research: Annotated Sources

**Sprint data breaches**

**Resources:**

Abel, R. (2019, July 17). Sprint customer data breached via Samsung website flaw. Retrieved from <https://www.scmagazine.com/home/security-news/data-breach/sprint-is-notifying-customers-that-threat-actors-gained-unauthorized-access-to-an-undisclosed-number-of-customer-accounts-via-a-compromised-samsung-website/>

* Sprint said that the PIN may have been compromised. People were instructed to place a fraud alert on their credit reports. Sprint was criticized for not taking this breach seriously enough. Attackers are gaining info bit by bit and may eventually be able to do an account takeover with enough info. There was a 26.5 billion dollar merger about to take place with T-Mobile.

Amir, U. (2019, July 29). Hackers used Samsung website to access Sprint's customer data. Retrieved from <https://www.hackread.com/hackers-used-samsung-website-to-access-sprints-customer-data/>

* This site contains a link to the PDF that was sent to some Sprint customers. Sprint refers to the Federal Trade Commission to help consumers protect themselves against fraud. Sprint then provides 5 steps to keep their accounts protected.

Cimpanu, C. (2019, July 16). Sprint says hackers breached customer accounts via Samsung website. Retrieved from <https://www.zdnet.com/article/sprint-says-hackers-breached-customer-accounts-via-samsung-website/>

* Hackers used the add a line site to break into a number of Sprint accounts. Sprint was informed about this on June 22.The personal information that may have been view were phone number, device type, device ID, monthly recurring charges, subscriber ID, account number, account creation date, upgrade eligibility, first and last name, billing address and add-on services.

Fingas, J. (2019, July 16). Hackers broke into Sprint accounts through Samsung's website. Retrieved from <https://www.engadget.com/2019/07/16/sprint-samsung-account-data-breach/>

* Since this Sprint breach was through the Samsung website, the scale was limited.

Ikeda, Scott. (2019, July 25). Sprint Data Breach Exposes Customers to Unknown Attackers; Will This Impact the T-Mobile Merger?. Retreived from <https://www.cpomagazine.com/cyber-security/sprint-data-breach-exposes-customers-to-unknown-attackers-will-this-impact-the-t-mobile-merger/>

* Sprint sent out notifications mid-July while the attack happened mid-June. There was a prior data breach through Boost mobile that people were notified about in May. PINs were compromised through the Boost mobile attack. This site also gives a summary of the impact this might have with the T-Mobile merger.

Mathews, L. (2019, July 17). Sprint Customer Data Exposed After A Samsung Website Gets Hacked. Retrieved from <https://www.forbes.com/sites/leemathews/2019/07/17/sprint-customer-data-exposed-after-a-samsung-website-gets-hacked/#472add4a16ab>

* Backdoor was found to Sprint’s database through the Samsung website. “It's quite possible that the passwords for those impacted accounts were sourced from previous breaches.” This hack could bring phishing attacks that use the information that was breached.

Reichert, C. (2019, July 16). Sprint customer details have been hacked. Retrieved from <https://www.cnet.com/news/sprint-customer-accounts-breached-by-hackers/>

* Sprint believes that they haven't found any fraudulent activity as a result of the breach. Sprint notified their customers on June 25.Credit card numbers and social security numbers were encrypted and not compromised.

Security Experts. (2019, July 18). Telecoms Giant Sprint Suffers Data Breach via Samsung Website. Retrieved from <https://www.informationsecuritybuzz.com/expert-comments/telecoms-giant-sprint-suffers-data-breach-via-samsung-website/>

* This site has many “security experts” give a quick note on the matter. It took a minimum of 3 days to get the breach under control.

Sprint Confirms Data Breach for Second Time in 2019. (2019, October 21). Retrieved from <https://www.securitymagazine.com/articles/90560-sprint-confirms-data-breach-for-second-time-in-2019>

* “Sprint says it ‘re-secured’ the customer's account if they received a notification that the account PIN had been reset”.

**Outline**

* **Sprint hacks summaries**

General overview of this hack

H[ackers used Boost phone numbers and Boost.com PIN codes](https://www.scribd.com/document/417811438/Sprint-breach-notification-Boost-Mobile) to access users' Sprint accounts.

Hackers first started accessing Sprint accounts via the Samsung.com website.

CNET sister site ZDNet report

PIN reset

* **The Sprint data breach**

How it all started

Boost Mobile breach

Samsung’s public-facing website was breached

Customer PINs compromised

* **The Sprint Security Concerns**

SIM swap attacks

Sam Bakken, Senior Product Marketing Manager

Craig Young, computer security researcher

Bypassing SMS based 2-factor authentication.

* **Clouds over the T-Mobile merger? ·**

T-Mobile and Sprint merger

5G network

Encrypted passwords exposed in a data breach

* **Second breach, Sprint did not take first breach seriously?**

Sprint Confirms Data Breach for Second Time

Hackers broke into customer accounts via the Samsung.com "add a line" website.

The personal information Exposed.

* **How were these vulnerabilities mitigated**

# Backdoor found by cybercriminals

Re-use passwords

Phishing attacks

Samsung biggest Sprint supplier hacked

* **Impact and implications of this attacks**

PIN compromised

Threat actors and unauthorize access

Sprint resecured customer accounts

Sprint announced that it lost 189,000 customers

Bitglass Chief Technology Officer (perspective)

* **Sprint resolution**

Re-secured all compromised accounts by resetting PIN codes

A smart VPN for mobile devices ( keeping customer from becoming pawns in a Wi-Fi hacker’s game)