

# Podcast Script

## INTRO

**Person 1:** "Magandang araw sa inyong lahat! Welcome sa ating podcast tungkol sa cybersecurity. Today, pag-uusapan natin ang isa sa pinakamalaking data breaches sa kasaysayan—ang 2019 Facebook Data Leak. Grabe, higit 530 milyong users ang naapektuhan!"

**Person 2:** "Oo nga! Isipin mo, isang araw, bigla mo na lang malalaman na kumakalat na sa internet ang phone number, pangalan, email, at lokasyon mo. Ang lala!"

**Person 3:** "Kaya nga! Pero paano ba nangyari 'to? Anong butas sa security ang ginamit ng hackers? At ano ang dapat nating matutunan dito?"

## SECTION 1: Anong Vulnerability ang Inexploit ng Hackers?

**Person 4:** "Ganito kasi 'yun. May butas sa 'Contact Importer' feature ng Facebook. Ginamit ng hackers ang automated tools para i-link ang phone numbers sa Facebook accounts. Sa madaling salita, parang in-scrape nila ang data nang hindi namamalayan ng Facebook."

**Person 5:** "Tama! At kahit inayos na ito ng Facebook noong August 2019, huli na ang lahat—kumalat na ang data sa hacker forums noong 2021. At guess what? Libre nilang pinamigay!"

**Person 6:** "So, technically, hindi ito hacking ng mismong Facebook servers. More on mass data scraping gamit ang loophole sa security system nila."

## SECTION 2: Paano Nakaapekto sa Confidentiality, Integrity, at Availability (C.I.A.)?

**Person 1:** "Pag-usapan natin ang epekto nito sa tinatawag na C.I.A.—Confidentiality, Integrity, at Availability."

**Person 2:** "Unang-una, ang confidentiality. Syempre, exposed na ang personal info ng mga tao. Madali na silang mabiktima ng phishing, scams, at identity theft."

**Person 3:** "Sa integrity naman, hindi naman nagalaw ang mismong Facebook accounts, pero puwedeng gamitin ang data sa panloloko, tulad ng impersonation at social engineering."

**Person 4:** "At sa availability, hindi naman naapektuhan ang mismong Facebook, pero delikado kasi nagamit ng hackers ang data para sa cyberattacks."

## SECTION 3: Paano Sana Napigilan ang Pag-leak ng Data?

**Person 5:** *"Eto na ang tanong—paano sana napigilan 'to?"*

**Person 6:** *"Una, dapat mas mahigpit ang rate-limiting ng Facebook para hindi basta-basta makapag-scrape ng data ang bots."*

**Person 1:** *"Tama! Dapat din encrypted ang phone numbers para kahit manakaw, hindi madaling magamit."*

**Person 2:** *"At higit sa lahat, dapat may mas mahigpit na kontrol sa API security para hindi madaling makuha ang user information."*

## SECTION 4: Ano ang Dapat Gawin ng Users at Mga Kumpanya?

**Person 3:** *"So, anong dapat nating gawin bilang users para maprotektahan ang data natin?"*

**Person 4:** *"Una, siguraduhin nating naka-private ang personal info natin sa Facebook settings."*

**Person 5:** *"Pangalawa, huwag gumamit ng iisang email o phone number sa lahat ng accounts natin."*

**Person 6:** *"Pangatlo, mag-ingat sa phishing. Huwag basta-basta mag-click ng links na mukhang suspicious."*

**Person 1:** *"At para naman sa mga Company tulad ng Facebook, dapat maging transparent sila kapag may data breach. Dapat automatic na ina-alert ang mga users para makapag-ingat agad."*

## CONCLUSION

**Person 2:** *"So, ano ang lesson natin dito? Walang social media platform na 100% safe. Dapat laging aware tayo sa security ng data natin!"*

**Person 3:** *"Tama! Hindi lang dapat Facebook o ibang tech companies ang nag-iingat—tayo mismong users, kailangan din nating gawin ang part natin."*

**Person 4:** *"At 'yan ang discussion natin today! Salamat sa pakikinig, and remember—stay safe online!"*

*References:*

*After Data Breach Exposes 530 Million, Facebook Says It Will Not Notify Users : NPR*

*Failbook: Personal data of roughly 530 million accounts from 106 countries leaks online - NotebookCheck.net News*

*What Really Caused Facebook's 500M-User Data Leak? | WIRED*