**CEP146NDD Slides**

## **Slide 1 – Title**

**Title:**  
 **Mass Credential Exposure: Apple, Google, Facebook Case Study**

**Subtitle:**  
 Group Presentation – CEP146NDD

**Speaker Notes:**  
 Introduce the topic and mention this presentation covers a 16-billion credential leak, its impact, and the shift toward password-less authentication.

## **Slide 2 – Objective**

**Content:**

* Research a major event in software development: a massive credential leak (16B credentials).
* Understand **risks, implications**, and the **transition to password-less systems**.

**Speaker Notes:**  
 We’re focusing on what happened, how it affects users and developers, and the industry’s response.

**NOTE:** Slide 2’s optional, don’t have to add if you don’t want to.

## **Slide 3 – What Happened**

**Title:** The 16-Billion Credential Leak

**Content:**

* Discovered in **June 2025** across ~30 datasets on the **dark web**.
* **Apple, Google, Facebook** not hacked directly — their users’ data appeared in compilations.
* **85%** from **infostealer malware**, **15%** from **older breaches**.
* Example format: <https://facebook.com> : [jsmith@example.com](mailto:jsmith@example.com) : Databr3achFUd!

**Speaker Notes:**  
 Explain that this was not a single hack, but an aggregation of stolen data from various sources.

## **Slide 4 – Risks & Implications**

**Content:**

* **Credential stuffing:** reuse of stolen credentials.
* **Identity theft & fraud.**
* **Phishing campaigns** using leaked info.
* **Operational costs** for investigations & compliance.
* **Loss of user trust** and brand damage.

**Speaker Notes:**  
 Highlight that even unaffected companies face backlash when their users’ data appears in leaks.

## **Slide 5 – Developer & Design Lessons**

**Content:**

* **Never store plain text passwords.**
* Use strong **hashing (bcrypt, Argon2)** + salts.
* Enforce **MFA**.
* Integrate **breach-detection APIs** (e.g., *Have I Been Pwned*).
* Encourage **password managers**.
* Apply **secure coding practices** (validation, encryption, session limits).
* Educate users through clear design.

**Speaker Notes:**  
 This slide focuses on what developers can learn and implement to prevent similar issues.

## **Slide 6 – Password-less / Passkeys**

**Content:**

* Rise of **password-less sign-ins** (Microsoft, Google).
* **550% increase** in passkey use (Bitwarden, 2024).
* **More secure** and **user-friendly** than OTPs.
* **Device-bound vs synced passkeys:**
  + Device-bound → more secure.
  + Synced → more convenient.

**Speaker Notes:**  
 Discuss how this shift aims to remove passwords entirely, improving both security and UX.

## **Slide 7 – Criticism & Balanced View**

**Content:**

* **Inflated numbers:** duplicates and recycled data.
* Mostly from **older breaches**, not new hacks.
* It still exposes **systemic weaknesses** in password security.
* Stresses need for **user awareness** and **transparent reporting**.

**Speaker Notes:**  
 Reinforce that even if the numbers are overstated, the event still reveals serious security flaws.

## **Slide 8 – Summary**

**Content:**

* **16 billion credentials** exposed from malware + old breaches.
* Major risks: **credential stuffing, identity theft, phishing, trust loss.**
* Developers: adopt **hashing, MFA, passkeys, breach detection**.
* Password-less methods = future of authentication.

**Speaker Notes:**  
 Wrap up the key takeaways in under a minute.

**NOTE FOR SLIDE 8**: Also optional like Slide 2.