Video #721

Resources by Dhruv Rathee

Sr. No.	Statement	Source	Link to Source
1	क्या आप जानते हैं कि आपका password अभी internet पर Leak हो चुका है ? June 2025 में अब तक का सबसे बड़ा data leak सामने आया है, जिसमें Apple, Google Facebook, Instagram, accounts leak हो चुके हैं	Forbes 30th June 2025	https://www.forbes.com/sites/emilsayegh/2025/06/30/silent-breach-exposes-16-billion-passwords-5-things-you-must-do-now/
2	ये data मिला website Cybernews की एक investigation में। Cybernews की team 2025 की शुरुआत से ही data leak के लिए dark web को closely monitor कर रही थी।	Cyber News 30th June 2025	https://cybernews.com/security/billions-credentials-exposed-infostealers-data-leak/
3	उसे June तक 30 ऐसे datasets मिले	Forbes 30th June 2025	https://www.forbes.com/sites/emilsayegh/2025/06/30/silent-breach-exposes-16-billion-passwords-5-things-you-must-do-now/
4	जो किसी भी password या encryption से secured नहीं थे और इन्हें आसानी से access किया जा सकता था। इन 30 data sets में थीं 16 billion login details.	Cyber News 30th June 2025	https://cybernews.com/security/billions-credentials-exposed-infostealers-data-leak/

Sr. No.	Statement	Source	Link to Source
5	किसी को नहीं पता कि इस data को किसने इकट्ठा किया? cybercriminals ने, जो stolen data को collect कर रहे हैं या security researchers ने जो data breach को monitor करते हैं। ये datasets बहुत कम वक्त के लिए password या encryption के बिना exposed थे, जिससे यह पता नहीं लगा कि इन्हें कौन control कर रहा है। अगर किसी cybercriminal के पास ये 16 billion passwords हैं तो इनकी मदद से बहुत कुछ unprecedented किया जा सकता है। आपकी identity चोरी करके इसका misuse किया जा सकता है, या आपको blackmail भी किया जा सकता है।	Cyber News 30th June 2025	https://cybernews.com/security/billions-credentials-exposed-infostealers-data-leak/
6	इनमें सबसे पहला तरीका है phishing. इसमें attacker किसी user को trick करता है ताकि वह अपनी personal जानकारी खुद ही reveal कर दे, जैसे कि password, OTP, या credit card details। आमतौर पर phishing email, SMS या fake website के ज़रिए किया जाता है।	Cyber News 14th July 2022	https://cybernews.com/security/phishing-explained-from-fake-court-summons-to-forged-corporate-documents/
7	इसी तरह दूसरा तरीका है- credential stuffing. जिसमें attackers पुराने leaked usernames और passwords को दूसरे websites पर try करते हैं. ये usernames और passwords पहले कभी किसी data breach में सामने आ चुके होते हैं। यह इस assumption पर based होता है कि user ने हर जगह एक ही password रखा होगा।	CNN Business 7th May 2020	https://edition.cnn.com/2020/05/06/tech/data-breach-passwords-protection

Sr. No.	Statement	Source	Link to Source
8	Credential stuffing इसलिए successful होता है क्योंकि बहुत सारे लोग हर जगह एक ही password reuse करते हैं।	CNN Business 7th May 2020	https://edition.cnn.com/2020/05/06/tech/data-breach-passwords-protection
9	तीसरा तरीका होता है, Password spraying. यह एक ऐसी hacking technique है जिसमें attackers एक ही common password को बहुत सारे usernames पर आज़माते हैं। यह इसलिए किया जाता है क्योंकि ज्यादातर systems कुछ failed login attempts के बाद account को temporarily lock कर देते हैं, लेकिन password spraying में attacker हर account पर सिर्फ एक या दो बार login try करता है, जिससे detection और lockout से बचा जा सकता है।	Beyond Trust	https://www.beyondtrust.com/resources/glossary/password-spraying
10	चौथा तरीका है Brute Force. इसमें attackers अलग-अलग passwords try करके देखते हैं कि इनमें से क्या सही हो सकता है। Brute force का मतलब है हर possible combination को try करना। जैसे आपने वो suitcase देखा होगा जिसपर एक 3-digit number lock होता है, आगर आपको इसका password नहीं पता तो इसे खोलने के लिए आपको 000 से 999 तक के हर number को try करना पड़ेगा।	Cybernews 28th April 2025	https://cybernews.com/security/what-is-a-brute-force-attack/

Sr. No.	Statement	Source	Link to Source
11	लेकिन specialized software से hackers per second millions और कभी-कभी billions passwords try कर सकते हैं। Brute force method बहुत ज्यादा efficient नहीं होता क्योंकि ज्यादातर बड़े platforms कुछ failed attempts के बाद ही account को lock कर देते हैं। लेकिन जहां ये limit ना हो या passwords weak हों, वहां brute force से account hack होने की possibility ज्यादा रहती है। common passwords तो ऐसे attacks से seconds में crack हो जाते हैं।	Cyber News 28th April 2025	https://cybernews.com/security/what-is-a-brute-force-attack/
12	कुछ ऐसी चीजें हैं, जो data theft में hackers की मदद करती हैं। आजकल online companies हमारा data तो खूब collect करती हैं, लेकिन इसे अच्छे से secure नहीं कर पातीं, जिससे एक साथ लाखों-करोड़ों लोगों का data leak हो जाता है। जो individual data leak से बहुत ज्यादा खतरनाक होता है।	Vox 21st April 2022	https://www.vox.com/the-goods/23031858/data-breach-data-loss-personal-consequences

Sr. No.	Statement	Source	Link to Source
13	Password, strong है या weak, इसके पीछे पूरा एक science होता है। Passwords की strength measure होती है entropy में। जो password जितना unique, random और लंबा होगा, उसकी entropy उतनी ज्यादा होगी और brute force जैसे तरीकों से उसे crack करना उतनी ही मुश्किल। किसी भी password की entropy निकालने का एक mathematical formula होता है, जो कुछ इस तरीके का होता है- Entropy (in bits) = log2(N^L) The log base 2 of N raised to the power L इसमें L length of password होती है और N, एक set में possible character हैं, सिर्फ small letters, a-z: N = 26 small letters + number (a-z, 0-9): N = 26 + 10 = 36 small letters + capital letters + number (a-z, A-Z, 0-9): N = 26 + 26 + 10 = 62	Medium 22nd September 2023	https://medium.com/@sp00ky/bits-of-security-understanding-password-entropy-cb083888f57e
14	जिन passwords की entropy 25 bits से कम होती है, वे बहुत weak password माने जाते हैं। इसी तरह 25 से 50 bits entropy वाले passwords, weak, 50 से 75 वाले ठीक-ठाक और 75 से 100 वाले बहुत अच्छे और 100 bits से ज्यादा entropy वाले passwords excellent माने जाते हैं।	Medium 14th November 2021	https://medium.com/asecuritysite-when-bob-met-alice/password-entropy-826b3be47261

Sr. No.	Statement	Source	Link to Source
15	अगर हम India में सबसे ज़्यादा use किए जाने वाले 10 passwords को देखें तो इसमें पहले number पर 123456, दूसरे पर password, तीसरे पर 12345678, चौथे पर 123456789, पाँचवे पर abcd1234, छठे पर 12345, सातवें पर qwerty123, आठवें पर 1234567890, नौवें पर india123, और दसवें पर 1qaz@WSX हैं। (Link> India from dropdown) इनमें से शुरू के 8 passwords को crack करने में 1 second से भी कम समय लगेगा, india123 को 50 seconds और 1qaz@WSX को crack करने में 11 मिनट।	Nord Pass	https://nordpass.com/most-common-passwords-list/
16	इसी तरह US में सबसे common password 'secret' है।	Nord Security 13th September 2024	https://nordsecurity.com/press-area/americans-most-common-password-is-secret-
17	Two-factor authentication में account को access करने के लिए 2 तरीके का identification देना पड़ता है। ये 2 identification होते हैं- ऐसा कुछ जो आपको पता हो, (something you know) जैसे कि password और ऐसा कुछ जो आपके पास हो (something you have), जैसे कि phone या app पर message या fingerprint.	Investopedia 10th April 2024	https://www.investopedia.com/terms/t/twofactor-authentication-2fa.asp