Security Newsletter
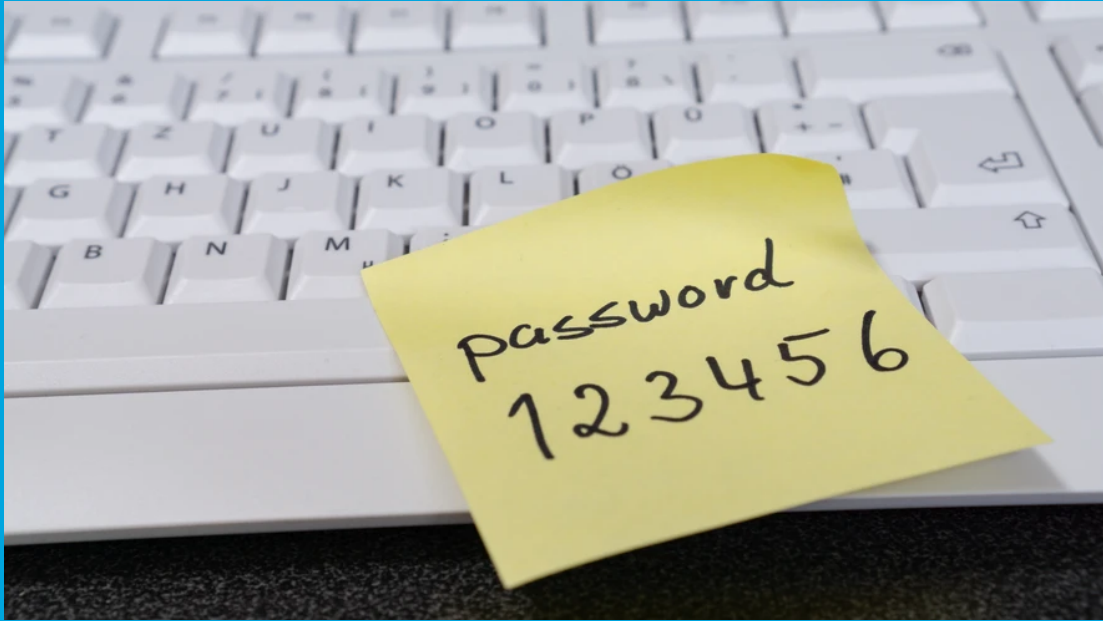
29 Nov 2021

It's 2021 But People are Still Using These Dumb Passwords

You would imagine that with most of our lives having moved online in these panoramic times, and with a sharp increase in news of someone, somewhere getting hacked, we would be a little more cautious about what our sacred passwords are.

Unfortunately, a list of the most common passwords in 2021 put out by NordPass will leave you with little hope for humanity. The top-of-the-class honours went to the password "123456," having been used 103,170,552 times.

Next in line was "123456789," which meets the eight character minimum requirement, but not much else in terms of actual security. Apart from more highly hackable number combinations, the top 10 list also has "password" and "qwerty" on it. All of these would take less than a second to breach.

Read More on Vice

Even More on NordPass

More #News

- Huge fines and a ban on default passwords in new UK law
- Apple sues NSO Group to curb the abuse of state-sponsored spyware
- The Internet is Held Together With Spit & Baling Wire
- Arrest in 'Ransom Your Employer' Email Scheme
- Google, Apple fined by Italian authority for aggressive data collection
- Interpol arrests over 1,000 suspects linked to cyber crime

- Hackers exploit Microsoft MSHTML bug to steal Google, Instagram creds
- Threat actors find and compromise exposed services in 24 hours
- FBI warns of phishing targeting high-profile brands' customers
- Biometric auth bypassed using fingerprint photo, printer, and glue
- Hackers Using Compromised Google Cloud Accounts to Mine Cryptocurrency
- What Avengers Movies Can Teach Us About Cybersecurity
- How the pandemic pulled Nigerian university students into cybercrime
- North Korean hackers posed as Samsung recruiters to target security researchers

#Breach Log

- Panasonic discloses data breach after network hack
- Marine services provider Swire Pacific Offshore hit by ransomware
- GoDaddy data breach hits WordPress hosting services resellers
- Over nine million Android devices infected by info-stealing trojan
- UK govt warns thousands of SMBs their online stores were hacked
- GoDaddy data breach hits 1.2 million Managed WordPress customers
- Wind turbine giant Vestas' data compromised in cyberattack

#Patch Time!

- New Windows 10 zero-day gives admin rights, gets unofficial patch
- Exploit released for Microsoft Exchange RCE bug, patch now
- VMware Warns of Newly Discovered Vulnerabilities in vSphere Web Client

#Tech and #Tools

- Insulet OmniPod Insulin Management System vulnerability
- WordPress Plugin Confusion: How an update can get you pwned
- How to Detect Azure Active Directory Backdoors: Identity Federation
- Abusing Windows Server Update Services (WSUS) to Enable NTLM Relaying Attacks
- Unlocking the Vault :: Unauthenticated Remote Code Execution against CommVault Command Center

This content was created by . Please share if you enjoyed!

Kindred Group in brief

Kindred Group is one of the world's leading online gambling operators with business across Europe, US and Australia, offering 30 million customers across 9 brands a great form of entertainment in a safe, fair and sustainable environment. The company, which employs about 1,600 people, is listed on Nasdaq Stockholm Large Cap and is a member of the European Gaming and Betting Association (EGBA) and founding member of IBIA (Sports Betting Integrity Association). Kindred Group is audited and certified by eCOGRA for compliance with the 2014 EU Recommendation on Consumer Protection and Responsible Gambling (2014/478/EU). Read more on www.kindredgroup.com.

You can access the previous newsletters at https://news.infosecgur.us