Another Data Breach, Another Reminder

If it feels like data breaches are becoming routine, you're not wrong. A recent report revealed that approximately 48 million Gmail usernames and passwords were found circulating online. The data appears to have come from a mix of past breaches, malware infections, and credential-stealing attacks rather than a single hack of Google itself, but the result is the same, a large number of real login details exposed and available to criminals.

When credentials like these are leaked, they're often used for more than just email access. Attackers know people reuse passwords, so stolen Gmail logins can be tested against banking sites, social media accounts, shopping accounts, and cloud services. Even if nothing looks wrong today, exposed credentials can be stored and used months, or even years later. Unfortunately, data theft doesn't always come with flashing warning lights.

Why Reusing Passwords Makes Things Worse

Password reuse is what turns a single breach into a much bigger problem. If the same password is used for email, social media, and financial accounts, one leak can unlock them all. This is why attackers love credential lists. They don't need to "hack" anything if people have already done the hard work for them. Using a password manager can help break this habit by creating and storing strong, unique passwords for every account. Tools like NordPass (from NordVPN) securely manage your logins so you don't have to remember dozens of passwords or reuse the same one everywhere. It's one of the simplest upgrades you can make to dramatically reduce risk. Click the link to NordVPN in the newsletter if you are interested. Next week we will report on how effective NordVPN is.

The first thing everyone should do is check whether their email address has appeared in known breaches. A free and trusted resource for this is *haveibeenpwned.com*, which allows you to safely check your email address against breach databases. If your email shows up, don't panic but do act. Think of it less like locking the barn after the horse escaped, and more like making sure no other doors were left wide open.

Quick Response Checklist: What to Do After a Breach

☐ Check your email address at haveibeenpwned.com
☐ Change your email password immediately
☐ Change passwords anywhere the same password was reused
☐ Enable two-factor authentication (2FA) on important accounts
☐ Review account activity for anything unusual
☐ Consider using a password manager to prevent future reuse

Bottom line:
One strong, unique password per account beats one "great" password everywhere.