



DEER BROOK

CYBER | TECHNOLOGY | SOLUTIONS

Work Accounts and Personal Accounts: Don't Mix and Match



When using the Internet, it's inevitable that you'll accumulate personal accounts for social media, shopping, banking, email, and more. Each one of these accounts often requires an email address during registration, and sometimes these addresses will even be our account usernames on these websites.

But sometimes, employees register on these websites using their work email and password. This is a huge problem businesses face, that puts both the business and the employee at risk.

Passwords: a necessary pain in the behind

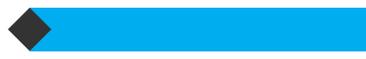


Let's face it; juggling dozens of different passwords is a pain in the butt. And over the years, password requirements have only gotten more complex. Not to mention that we're sometimes forced to change our passwords from seemingly out of nowhere.

So, by reusing the same passwords across multiple accounts, we make our lives a bit easier.

However, we make a scammer's life easier too.

A typical data breach: what happens, exactly?



Let's take that shopping site from the beginning of our example, and let's say they get hacked. What happens next?

Without a doubt, your username, email address, password and other information has been breached. In turn, that information is going to wind up in collection databases across the dark web; these databases can contain over 700 million email addresses and usernames.

Hackers will pay to access these databases and will check to see if there's any email addresses ending in corporate domains. When they find some, they run those addresses and passwords against online email and work portals, checking to see if the user had, in fact, used the same password for their personal account and work account.

Passwords that aren't periodically reset and passwords that are reused across multiple websites are at risk to be used by bad actors to scratch and claw their way towards sensitive, protected data.



Even if your passwords aren't the same, and even if you don't use a work email for a personal account, you've likely already been a victim of a data breach and have your account information out there, somewhere, in some giant collection.

Account breaches: what do I do from here?



To see if your email address has been involved in a data breach, visit the website www.haveibeenpwned.com and check. Even if your email address doesn't come up in its search, you should still exhibit good personal security habits and assume that it has, or that it will.

Wrapping up



If you discover your email address has been involved in a data breach, the best thing to do is change your passwords not only for one specific breached account, but all your other online accounts that use the same email as well.

deer-brook.com



DEER BROOK

CYBER | TECHNOLOGY | SOLUTIONS

