GoodSuite
Speed • Innovation • Technology

6. Latest 22 Dark Web Breach Details

February/2022

GoodSuite
Speed • Innovation • Technology

4 dijo@abcco.com

Date	Account Breached	Data Exposed
2020-10-21	Mixed Credential and PII Dump - July 2020 - internal.labase.org	
2019-12-19	The 2844 Collection - internal.labase.org	
2018-03-15	internal.labase.org.txt solenya collection leak	

5 jsmith@abcco.com

Date	Account Breached	Data Exposed
2020-06-19	LeadHunter_Part-32	address,email,ip address,name,phone
2019-12-28	The 2844 Collection - evony.com	
2017-11-01	Onliner Spambot email list	email,password
2017-10-16	Evony game creds breach	password

6 123@abcco.com

Date	Account Breached	Data Exposed
2020-06-19	ExploitIN 800M - Part 38	email,password
2020-01-29	Big Asia Leak	address,email,password
2016-08-01	very large credential dump	
2015-08-18	Alleged AshleyMadison.com data breach release	address,email,login

Continue on the next page

7. Latest 22 Dark Web Breach Details

February/2022

GoodSuite
Speed • Innovation • Technology

7 abc@abcco.com

Date	Account Breached	Data Exposed
2020-06-17	ExploitIN 800M - Part 14	email,password
2016-08-01	very large credential dump	
2013-11-11	Adobe Hack	address,email,login,password

8 corinaperez@abcco.com

Date	Account Breached	Data Exposed
2020-06-17	ExploitIN 800M - Part 13	email,password
2016-08-01	very large credential dump	

9 jdoe@abcco.com

Date	Account Breached	Data Exposed
2020-06-17	ExploitIN 800M - Part 13	email,password
2019-06-24	Collections No. 1 Credentials Leak Deduped	
2016-08-01	very large credential dump	

10 jo@abcco.com

Date	Account Breached	Data Exposed
2020-05-13	PetFlow	address,email,password

Continue on the next page

8. Latest 22 Dark Web Breach Details

February/2022

GoodSuite
Speed • Innovation • Technology

11 trstaccount@abcco.com

Date	Account Breached	Data Exposed
2020-02-11	Zynga	address,email,password

12 a@abcco.com

Date	Account Breached	Data Exposed
2017-11-01	Onliner Spambot email list	email,password

13 jeff.smith@abcco.com

Date	Account Breached	Data Exposed
2017-11-01	Onliner Spambot email list	email,password

14 kim.williams@abcco.com

Date	Account Breached	Data Exposed
2017-11-01	Onliner Spambot email list	email,password

15 tim.jones@abcco.com

Date	Account Breached	Data Exposed
2017-11-01	Onliner Spambot email list	email,password

16 bm@abcco.com

Date	Account Breached	Data Exposed
2016-06-01	MySpace credentials dump	

Continue on the next page

9. Latest 22 Dark Web Breach Details

February/2022

GoodSuite
Speed • Innovation • Technology

17 amy.smith@abcco.com

Date	Account Breached	Data Exposed
2016-05-19	LinkedIn credentials dumped	address,email,password

18 REBECCA.SMITH@ABCCO.COM

Date	Account Breached	Data Exposed
2016-05-19	LinkedIn credentials dumped	address,email,password

19 sdawson@abcco.com

Date	Account Breached	Data Exposed
2016-05-19	LinkedIn credentials dumped	address,email,password

20 shane@abcco.com

Date	Account Breached	Data Exposed
2016-05-19	LinkedIn credentials dumped	address,email,password

21 fred@abcco.com

Date	Account Breached	Data Exposed
2016-03-11	Large credentials cache	email,password

22 user23@abcco.com

Date	Account Breached	Data Exposed
2015-08-18	Alleged AshleyMadison.com data breach release	address,email,login

Breached Passwords

When breached account credentials like email address and passwords become available on the dark web, they can be used to access that account, steal information, or access additional accounts that may use the same credentials.

Spear Phishing

Even if passwords weren't compromised on the dark web, the email address, physical address, or other personally identifiable information can be used to craft specific and convincing phishing emails that could put your business at future risk.

Network Access

If the credentials compromised are the same credentials used to access your business network or sensitive customer information, criminals could use this information for unauthorized access to your network where they can wreak havoc.

11. What Happens Now?

Someone at your organization had data exposed on the dark web… what happens now? Unfortunately, the impact of a third-party data breach involving your or one of your employee's business accounts could be a vulnerability to your business. Learn what you can do to proactively address these hidden threats

How can I **protect** my employees and my business.

We know this information can be alarming and quite frankly, scary, but it doesn't have to be! We share this information with you to keep you informed so you can proactively prevent this compromised information from coming back to harm your organization in the future. We strongly recommend that all impacted employees take the following steps towards remediation.

1.  **Update your password on the compromised account**

2.  **Be wary of an increase in phishing emails being sent to you.**

3.  **Avoid using your business email address for non-business activities and account management.**

4.  **Change the password for all accounts where this password may have been reused and remember to use strong, unique passwords for all your accounts**

Have **questions** or want more tips on best practices?

If you have questions on any of these results or how to proactively protect your employees and your business, please feel free to contact us!