YH ROCU

Yorkshire & Humber
REGIONAL CYBER CRIME UNIT

550 MILLION STOLEN USER RECORDS SOLD

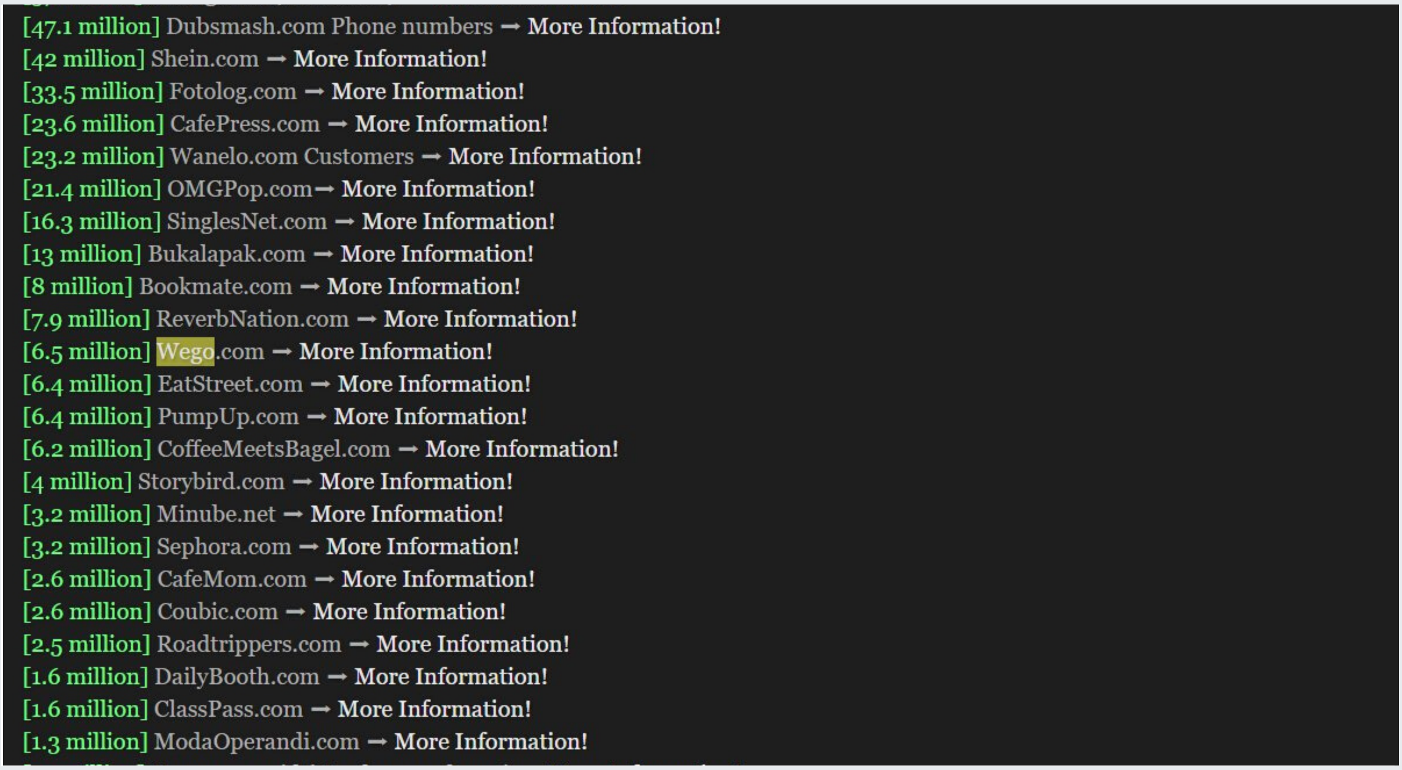
A threat actor is selling twenty-nine databases on a hacker forum that allegedly contains a combined total of 550 million stolen user records. Also, a database of 47.1 million phone numbers that were part of a 2018 Dubsmash data breach.

The threat actor began selling these databases on May 7th, when they posted them on a well-known site where threat actors can buy each one individually.

None of these data breaches appear to be new, with the oldest being from 2012 and the latest from last month. The volume of user accounts for sale is concerning as the information exposed could be used to perform large-scale credential stuffing or targeted phishing attacks.

Victims should remain vigilant and change their passwords where necessary. Ensure you implement MFA where possible and educate staff on password security and phishing. Further advice can be found at:

www.yhrocu.org.uk/departments/regional-cyber-crime-unit/protect/



[47.1 million] Dubsmash.com Phone numbers → More Information!
[42 million] Shein.com → More Information!
[33.5 million] Fotolog.com → More Information!
[23.6 million] CafePress.com → More Information!
[23.2 million] Wanelo.com Customers → More Information!
[21.4 million] OMGPop.com→ More Information!
[16.3 million] SinglesNet.com → More Information!
[13 million] Bukalapak.com → More Information!
[8 million] Bookmate.com → More Information!
[7.9 million] ReverbNation.com → More Information!
[6.5 million] Wego.com → More Information!
[6.4 million] EatStreet.com → More Information!
[6.4 million] PumpUp.com → More Information!
[6.2 million] CoffeeMeetsBagel.com → More Information!
[4 million] Storybird.com → More Information!
[3.2 million] Minube.net → More Information!
[3.2 million] Sephora.com → More Information!
[2.6 million] CafeMom.com → More Information!
[2.6 million] Coubic.com → More Information!
[2.5 million] Roadtrippers.com → More Information!
[1.6 million] DailyBooth.com → More Information!
[1.6 million] ClassPass.com → More Information!
[1.3 million] ModaOperandi.com → More Information!

BLUETOOTH SECURITY

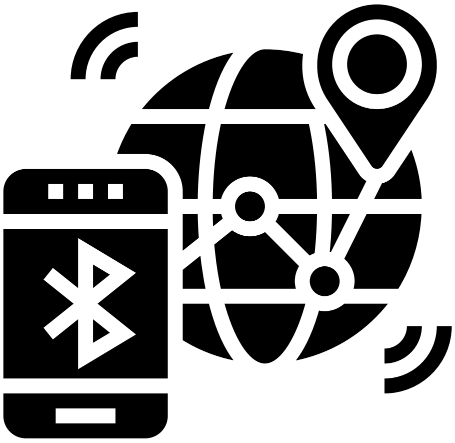
What Bluetooth offers:

• *Pair devices:* Allows individuals to connect various devices such as wireless speakers or make hands-free calls with mobile.
• *Share files:* Photos, videos and music can be sent between different devices. Fitness trackers and smart watches also use it to pair a mobile to the tracker.
• *Set up tethering*: If a computer does not have internet access and a phone does, it is possible to share this internet connectivity.

Security concerns
The more dangerous Bluetooth attacks are uncommon due to the technical skills required to carry them out. The attacks require the victim to be in close proximity to the attacker for a sustained period of time.

• *Bluejacking* involves sending a 'business card' to another nearby user via text. The card can contain unsolicited messages, this is a nuisance rather than a security concern.
• *Bluesnarfing* is when the same business card is used to request a Bluetooth connection, then they can send malicious files or steal information leading to identity theft, social engineering or worse.
• *Bluebugging* allows hackers to take control of a mobile in order to make phone calls, send and read SMS, eavesdrop on phone conversations, and connect to the Internet.
• *Blueborne* attacks compromise a range of electronic devices. The hacker can assert control over each device or use them as a spring board to attack other devices.

Security solutions
• *Update devices:* Updates fix security weaknesses. Google and Amazon have already released patches for Blueborne attacks.
• *Secure connections*: Set the device to only connect with trusted devices and to require a pin code before establishing a new connection.
• *Turn your Bluetooth off:* When not in use, in crowded locations or whilst working with sensitive data.
• *Configure App permissions*: Limit your apps that utilise Bluetooth through the 'settings' menu. Turning off Airdrop, for example prevents your phone unwittingly sharing or receiving sensitive or configure settings to 'contacts only' mode



COVID-19 ACTION FRAUD REPORTS RECORDED AS OF 19 MAY 2020

Total reports to Action Fraud = 1,880
Total financial losses = £4,279,011
Total reports of phishing to Action Fraud = 10,037

(as of 27/4/20, includes figures from NCSC suspicious email reporting service)