Password and Security Breach Awareness

A hacker who was selling details of nearly 890 million online accounts stolen from 32 popular websites in three separate rounds has now put up a fourth batch of millions of records originating from 6 other sites for sale on the dark web.

The hacker is selling each of the above listed hacked databases individually on Dream Market for a total worth 1.2431 Bitcoin, that's roughly $5,000.

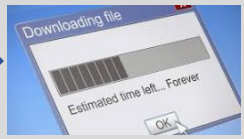
https://thehackernews.com/2019/03/data-breach-security.html

HOW DO THEY DO IT …

Research their target, person or company

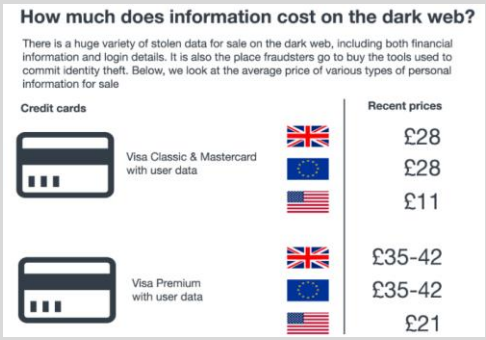
Connect to yahoo, paypal servers, hack admin accounts, get access to username and password tables

Download password list, this forms a file with list of names and password (generates a dictionary file)



They upload to dark web for sale

Personal Information Category	Average Value on Dark Web	Sales price explained
Paypal login	£279.74	By far the most commonly listed items. Sale prices tend to be worth around 10% of the available credit balance.
Online bank details	£167.81	
Passport	£39.76	Digital proof of identity can be used to setup lines of credit.
eBay login	£26.20	Allowing fraudsters to dupe buyers into sending them money for fake listings, and also buy expensive goods with the owner's funds to intercept and sell-on.
Netflix login	£5.99	A route to identity fraud, giving criminals the bonus of being able to stream content for free.
Uber login	£5.02	There have also been reports of Russians using hacked Uber accounts to run up big bills for Uber journeys the true owner has never taken, sometimes on the other side of the world.
Deliveroo login	£3.74	Fraudsters can use hacked food delivery accounts to order takeaways and drink - satiating their appetite for crime.
Skype login	£3.00	Compromised Skype accounts allow scammers to send 'phishing' links to trusted contacts.
Match.com login	£2.24	Stolen details can be used for 'catfishing', where you mimic a person's identity to engage in a relationship to exploit them financially.



They then have your username & passwords and can access your email, they can then contact companies you receive emails from (banks, shopping receipts), they can get legitimate statements or forms with address etc, they then can go to a bank and open an account in your name with the correct paper work.

Identity theft all from a username and password breach.

OTHER USED METHODS

Interception :- Listening between the two connections, WIFI is the easiest to see & capture

Key log software :- Send you an email ,you click on a link, it loads a piece of software in the background, it then captures your passwords and emails them to the sender.

Shoulder Surfing :- Similar to watching you put your pin code in for your bank card at cash Machine

Phishing :- Email you for your data using misconception, and social engineering

Brute force :- A file that has had new passwords added from previous breaches generating one big file, it is then used as brute force to login to a system and work its way down the password list.

Sticky notes :- staff leaving postits on desk, sellotape password to laptop !

HAS MY EMAIL AND PASSWORD I USE FOR YAHOO, SAINSBURY, BEEN LOCATED IN A DICTIONARY FILE ?????

Has my account been compromised (yahoo, Hotmail, paypal etc)?!?!

This is a unique website that allows you to check if any of your online usernames or email address show on any databases from previous breaches. If your listed, change the password to the account and any other accounts using the same password, do not add a number or change 1 letter, **change the whole password** and use the best practise below…

https://haveibeenpwned.com/

WHAT TO DO… if you have been Pwned

Best password practice

1. Use a very complex password 12 long (letters, numbers, symbols) don't use dictionary words, use a phrase and break down to characters. These are near on impossible to break unless you leave it written down !!. Remember the phrase and then use this for all accounts so only one complicated password to remember..
   PHRASE :- I love being in America and on the beach
   PASSWORD :- ILb1AA0Tb!

2. Use several phrases to create several passwords, then use a password software vault to store them so you don't have to remember them all just one to access the vault, then when you login with a password, it texts you a code for then to enter then code to authenticate, so 2 passwords to access your password list.

   Government advice to passwords https://www.ncsc.gov.uk/blog-post/passwords-passwords-everywhere
   IS your password on the list https://www.ncsc.gov.uk/static-assets/documents/PwnedPasswordTop100k.txt

3. Do not use the same password for your personal accounts for you work accounts !. They must be different.