



There is so much technology protecting our networks and computers now, that hackers go for the easy targets:

YOU



How people think they get hacked



How they really get hacked

Good Old Days
March 9 at 8:30am · 🌐

DO YOU REMEMBER YOUR FIRST GRADE TEACHERS NAME?



WHAT CAR DID YOU LEARN TO DRIVE STICK SHIFT ON?



Remember your first concert?
How old were you, and who did you see?



springchicken.co.uk ✓
February 6, 2017 · 🌐

What street did you grow up on? Where is the first address you remember living?
Let's see if we can put some Spring Chickens in touch with old friends?
Check out our shop at <http://www.springchicken.co.uk/>



Please Like and Share our Spring Chicken Facebook page

What's Your Elf Name?

First letter of your **first name:**

A- Sweetie	N- Cookie
B- Jolly	O- Sparkle
C- Bubbles	P- Cheerful
D- Tootsie	Q- Delightful
E- Joyful	R- Spunky
F- Sugarplum	S- Candy
G- Twinkle	T- Sprinkles
H- Candy	U- Cupcake
I- Merry	V- Perky
J- Flirty	W- Frosty
K- Chipper	X- Precious
L- Angelic	Y- Sunny
M- Happy	Z- Pinky

Your **Birth Month:**

January- TwinkleToes
February- Sugarplum
March- McJingles
April- SparklePants
May- PeppermintBuns
June- SugarSocks
July- SprinklePants
August- AngelEars
September- SugarBells
October- PointyToes
November- McSprinkles
December- JollyToes



👍❤️👍 1.5K 1K Comments 517 Shares

👍 Like 💬 Comment ➦ Share

N FILM

/the social dilemma

This documentary-drama hybrid explores the dangerous human impact of social networking, with tech experts sounding the alarm on their own creations.

"If you're not paying for the product, then you are the product" — Daniel Hövermann

"There are only two industries that call their customers 'users': illegal drugs and software." — Edward Tufte

Worth a watch!



The Normal Approach to Passwords

The password requirements are normally set to:

More than 8 characters

At least 1 number, 1 Special Character and 1 upper case letter

calculator

Start with a base word of your choice

calculator1

Add a number

calculator1!

Add a special character

Calculator1!

Add a Capital Letter

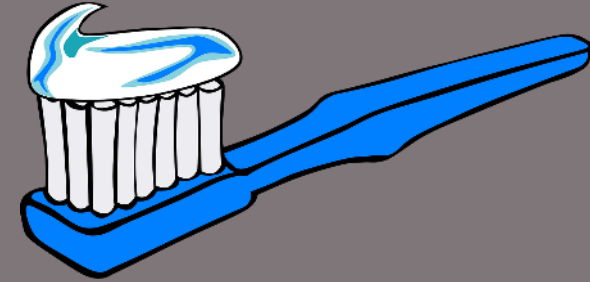
There's **not** a lot of difference from the original. It's still easy to guess.

Three Random Words

PensionerPowerAdvocate-4

PensionerPowerAdvocate-a4

Treat your Password *like a toothbrush*



1. Choose a good one.
2. Don't share it with anyone or use it for any other purpose.
3. Change it if you think someone has used it.

Use Multi-factor Authentication Where possible



Check if your online accounts have been hacked

Browse to <https://haveibeenpwned.com/>

Enter your email address and click -----

pwned?

haveibeenpwned is an online database of known compromised web accounts. It will list any of your accounts that have been hacked in the past. Review the list and be aware that the password used on the account/s have been made public and available to hackers around the world. Change the password, and if you have used the same email & password combination elsewhere, go change that as well, because the hackers would have tried that already.

Oh no — pwned!

Pwned in 10 [data breaches](#) and found no [pastes](#) ([subscribe](#) to search sensitive breaches)

3 Steps to better security

[Start using 1Password.com](#)



Step 1 Protect yourself using 1Password to generate and save strong passwords for each website.



Step 2 Enable 2 factor authentication and store the codes inside your 1Password account.



Step 3 Subscribe to notifications for any other breaches. Then just change that unique password.

[Why 1Password?](#)

    [Donate](#)

Breaches you were pwned in

A "breach" is an incident where data has been unintentionally exposed to the public. Using the [1Password password manager](#) helps you ensure all your passwords are strong and unique such that a breach of one service doesn't put your other services at risk.



Adobe: In October 2013, 153 million Adobe accounts were breached with each containing an internal ID, username, email, *encrypted* password and a password hint in plain text. The password cryptography was poorly done and many were quickly resolved back to plain text. The unencrypted hints also disclosed much about the passwords adding further to the risk that hundreds of millions of Adobe customers already faced.

Compromised data: Email addresses, Password hints, Passwords, Usernames



Apollo: In July 2018, the sales engagement startup Apollo left a database containing billions of data points publicly exposed without a password. The data was discovered by security researcher [Vinny Troia](#) who subsequently sent a subset of the data containing 126 million unique email addresses to Have I Been Pwned.

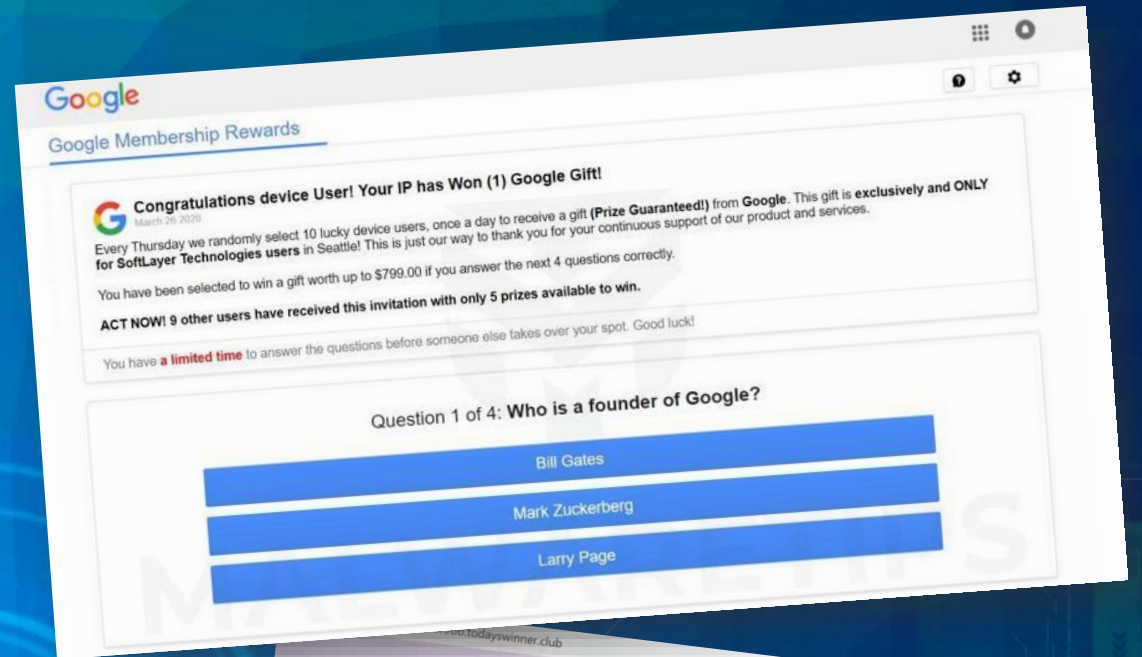


Quick TIP

Don't be fooled by Malvertising

Clicking a great sounding **BARGAIN** or a **FREE** iPhone is likely to end in you losing data or having your device infected.

THINK
Before You Click



Phishing Emails

Pay Pal
To: Me

< contctIT@paypall.com >

Hover over email addresses to check who they are really from



Customer,



Watch out for spelling and grammar errors

PayPal

We found incoorect information with your account and may lead to the immediate closure of your account
Click on the button below and update your info so fast and we thank you for your understanding and sorry for the inconvenience.

< http://give.me/your/info.com >

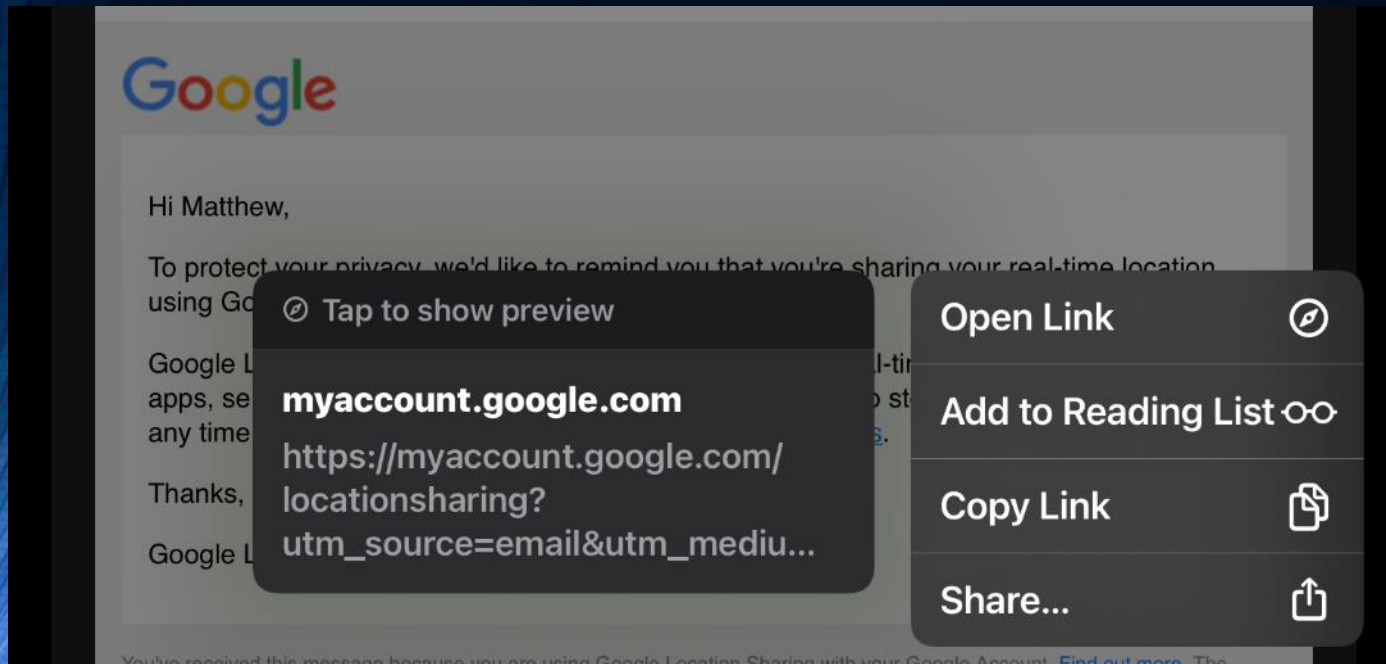
Click to Log in

Hover of links to check their real destination

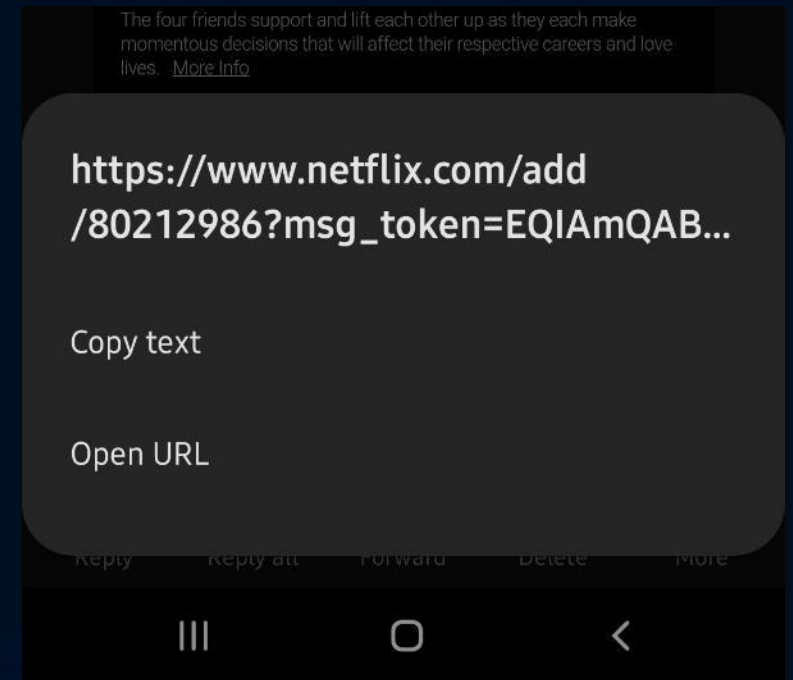


Checking links on Apple and Android Devices

When using a mobile device (with no mouse) you can *hold your finger down* on a link or email address and it will show you more detail.



Apple Devices



Android Devices

The effect of Artificial Intelligence on Social Engineering

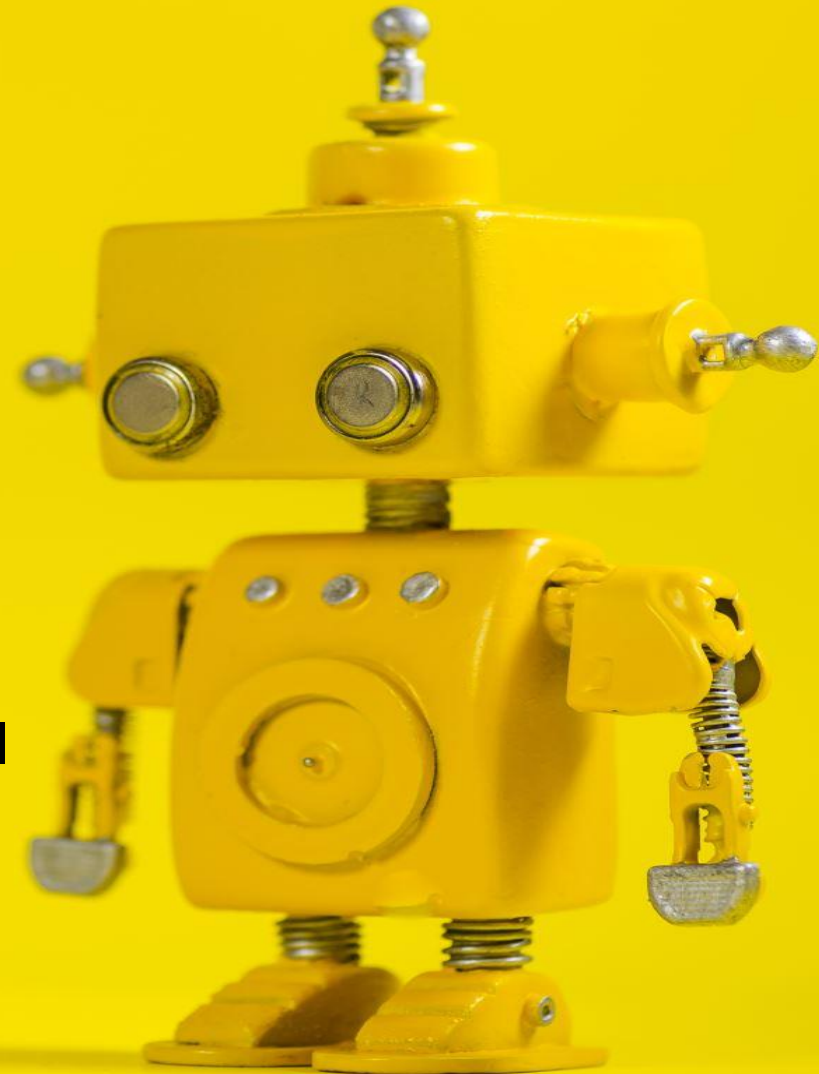
As AI gets better and more widely used, fraudsters will use it to improve their attacks.

Pros

- Improved Detection
- Enhanced Defence
- Automated Responses

Cons

- Sophistication of attacks
- No more spelling and grammar mistakes in phishing emails
- Our Privacy will be affected as AI manipulates human behaviour



Using Your Sixth Sense to Detect Red Flags

Be wary of unsolicited emails that request sensitive information or contain links or attachments.
Delete it!

Scammers often use scare tactics to pressure you into taking immediate action, such as threatening to close your account or demanding payment.
Ignore it!

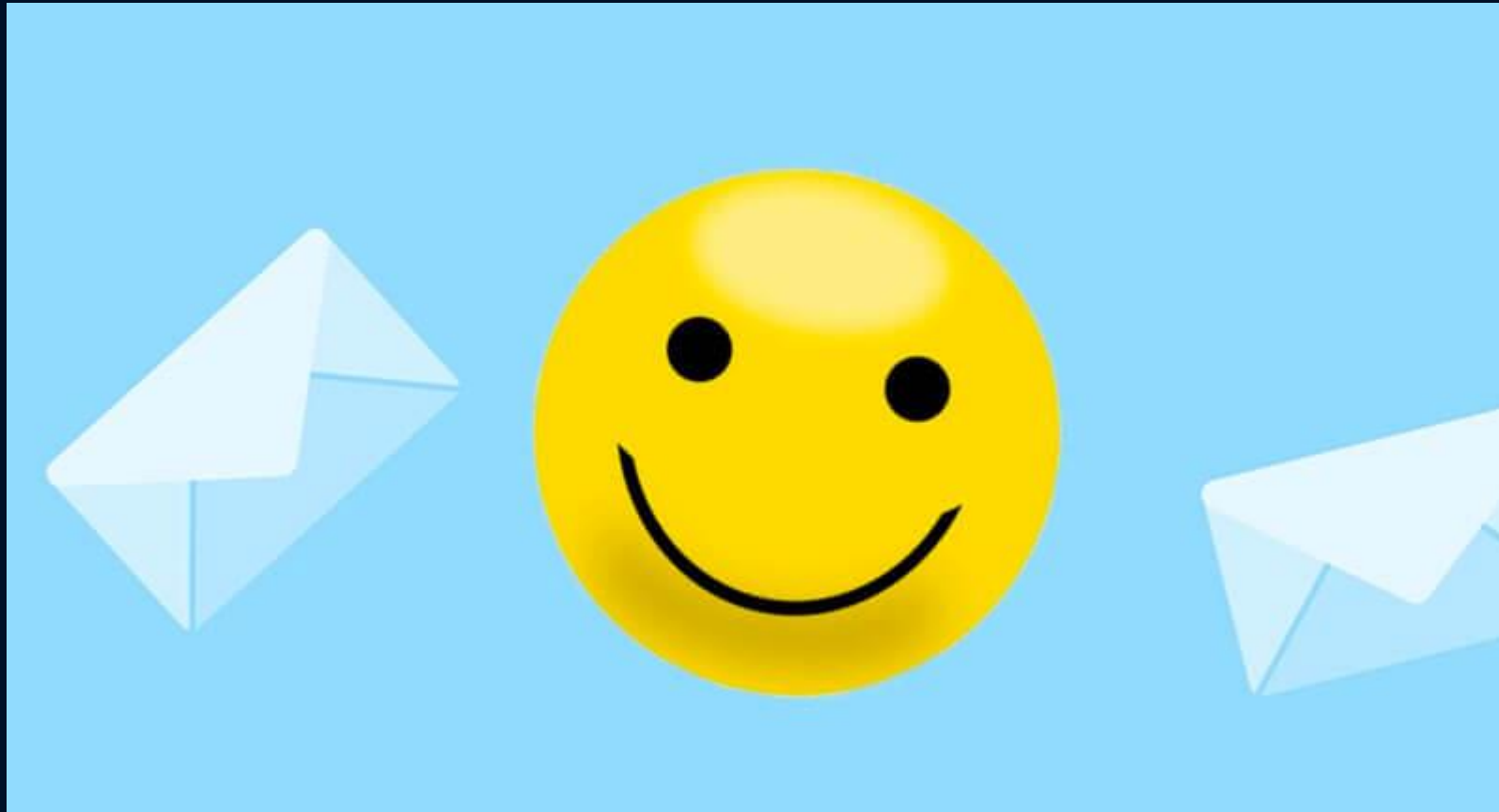
Always verify website before entering any personal or financial information. Check the address for errors or use a search engine to find the legitimate site. If in any doubt don't trust it!

Watch out for typos or grammatical errors in emails or on websites, as these can be indicators of a phishing scam. – Don't click it!

If something seems too good to be true, it probably is. Ignore it!

When in doubt, trust your gut. If something feels off or suspicious, don't take any chances.

How a missing smiley foiled a NZD \$90,000 email fraud



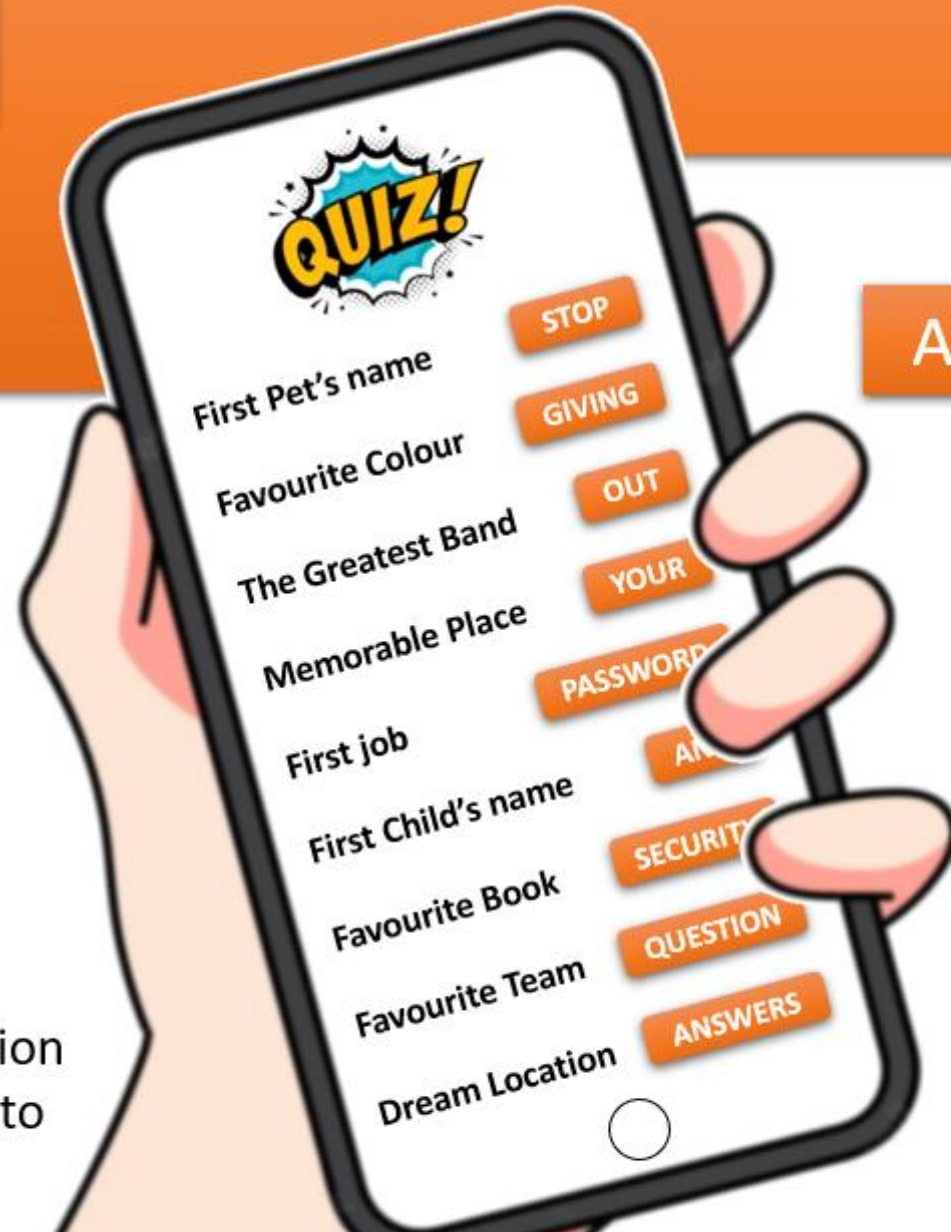
When a scammer's email left out a Smiley face on emails, this aroused suspicion in the mind of the assistant, because emails from this particular CEO normally contained exuberant flair such as smileys. This saved them NZD \$90,000

SCAM ALERT

Have you ever completed an online Quiz?

Sharing TOO MUCH personal information online could be dangerous!

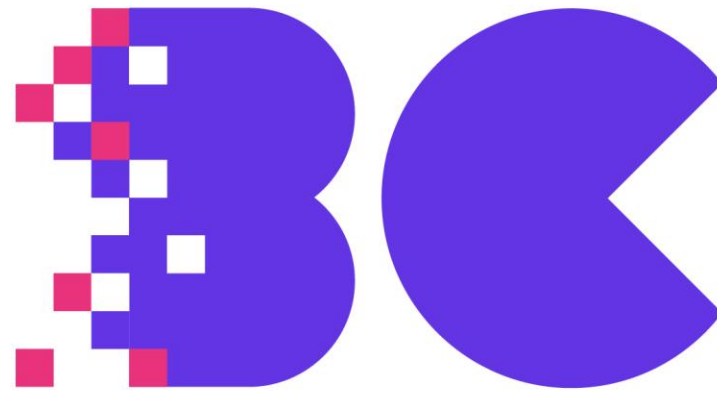
Cyber Criminals collect this information to guess your passwords and hack into your online accounts.



ARE YOU SCAM SAVY?

Scan the QR code and take the test!





TECHNOLOGIES

We Get IT

0330 800 1010

support@bc-group.co.uk