Cybr171 – Assignment 2
Thomas Green
greenthom – 300536064

1a.

Password: 123456

The test

Password to test: 123456 Break it down!

```
Estimating strength of password "123456" ...

Average number of guesses needed to crack: 2
Strength score (1-5): 1
WARNING: This is a top-10 common password
Suggestion 1: Add another word or two. Uncommon words are better.

Approx times to crack ...
   100/hour: 1 minute
  10/second: less than a second
 10k/second: less than a second
 10B/second: less than a second
```

```
How the password "123456" was broken into parts:

0:
  pattern: dictionary
  i: 0
  j: 5
  token: 123456
  matched_word: 123456
  rank: 1
  dictionary_name: passwords
  reversed: false
  l33t: false
  base_guesses: 1
  uppercase_variations: 1
  l33t_variations: 1
  guesses: 1
  guesses_log10: 0
```

How Secure Is My Password?

The #1 Password Strength Tool. Trusted and used by millions.

••••••

Your password would be cracked

Instantly

Test Your Password		Minimum Requirements
Password:	123456	• Minimum 8 characters in length • Contains 3/4 of the following items: - Uppercase Letters - Lowercase Letters - Numbers - Symbols
Hide:		
Score:	4%	
Complexity:	Very Weak	

Additions		Type	Rate	Count	Bonus
✗	Number of Characters	Flat	+(n*4)	6	+ 24
✗	Uppercase Letters	Cond/Incr	+((len-n)*2)	0	0
✗	Lowercase Letters	Cond/Incr	+((len-n)*2)	0	0
✓	Numbers	Cond	+(n*4)	6	0
✗	Symbols	Flat	+(n*6)	0	0
✓	Middle Numbers or Symbols	Flat	+(n*2)	4	+ 8
✗	Requirements	Flat	+(n*2)	1	0
Deductions					
✓	Letters Only	Flat	-n	0	0
!	Numbers Only	Flat	-n	6	- 6
✓	Repeat Characters (Case Insensitive)	Comp	-	0	0
✓	Consecutive Uppercase Letters	Flat	-(n*2)	0	0
✓	Consecutive Lowercase Letters	Flat	-(n*2)	0	0
!	Consecutive Numbers	Flat	-(n*2)	5	- 10
✓	Sequential Letters (3+)	Flat	-(n*3)	0	0
!	Sequential Numbers (3+)	Flat	-(n*3)	4	- 12
✓	Sequential Symbols (3+)	Flat	-(n*3)	0	0

Legend

✓ **Exceptional:** Exceeds minimum standards. Additional bonuses are applied.
✓ **Sufficient:** Meets minimum standards. Additional bonuses are applied.
! **Warning:** Advisory against employing bad practices. Overall score is reduced.
✗ **Failure:** Does not meet the minimum standards. Overall score is reduced.

Password: qwerty123

The test

Password to test: qwerty123 Break it down!

```
Estimating strength of password "qwerty123" ...

Average number of guesses needed to crack: 220
Strength score (1-5): 1
WARNING: This is a very common password
Suggestion 1: Add another word or two. Uncommon words are better.

Approx times to crack ...
   100/hour: 2 hours
  10/second: 22 seconds
 10k/second: less than a second
 10B/second: less than a second
```

```
How the password "qwerty123" was broken into parts:

0:
  pattern: dictionary
  i: 0
  j: 8
  token: qwerty123
  matched_word: qwerty123
  rank: 219
  dictionary_name: passwords
  reversed: false
  l33t: false
  base_guesses: 219
  uppercase_variations: 1
  l33t_variations: 1
  guesses: 219
  guesses_log10: 2.340444114840118
```

How Secure Is My Password?

The #1 Password Strength Tool. Trusted and used by millions.

•••••••••

Your password would be cracked

Instantly

Test Your Password		Minimum Requirements
Password:	qwerty123	• Minimum 8 characters in length • Contains 3/4 of the following items: - Uppercase Letters - Lowercase Letters - Numbers - Symbols
Hide:		
Score:	41%	
Complexity:	Good	

Additions		Type	Rate	Count	Bonus
✓	Number of Characters	Flat	+(n*4)	9	+ 36
✗	Uppercase Letters	Cond/Incr	+((len-n)*2)	0	0
✓	Lowercase Letters	Cond/Incr	+((len-n)*2)	6	+ 6
✓	Numbers	Cond	+(n*4)	3	+ 12
✗	Symbols	Flat	+(n*6)	0	0
✓	Middle Numbers or Symbols	Flat	+(n*2)	2	+ 4
✗	Requirements	Flat	+(n*2)	3	0
Deductions					
✓	Letters Only	Flat	-n	0	0
✓	Numbers Only	Flat	-n	0	0
✓	Repeat Characters (Case Insensitive)	Comp	-	0	0
✓	Consecutive Uppercase Letters	Flat	-(n*2)	0	0
!	Consecutive Lowercase Letters	Flat	-(n*2)	5	- 10
!	Consecutive Numbers	Flat	-(n*2)	2	- 4
✓	Sequential Letters (3+)	Flat	-(n*3)	0	0
!	Sequential Numbers (3+)	Flat	-(n*3)	1	- 3
✓	Sequential Symbols (3+)	Flat	-(n*3)	0	0

Legend

✓ **Exceptional:** Exceeds minimum standards. Additional bonuses are applied.
✓ **Sufficient:** Meets minimum standards. Additional bonuses are applied.
! **Warning:** Advisory against employing bad practices. Overall score is reduced.
✗ **Failure:** Does not meet the minimum standards. Overall score is reduced.

Password: ncc1071

The test

Password to test: ncc1071 Break it down!

```
Estimating strength of password "ncc1071" ...

Average number of guesses needed to crack: 5734000
Strength score (1-5): 3
WARNING: This is similar to a commonly used password
Suggestion 1: Add another word or two. Uncommon words are better.
Suggestion 2: Reversed words aren't much harder to guess

Approx times to crack ...
   100/hour: 6 years
  10/second: 7 days
 10k/second: 10 minutes
 10B/second: less than a second
```

```
How the password "ncc1071" was broken into parts:

0:
  pattern: bruteforce
  token: ncc
  i: 0
  j: 2
  guesses: 1000
  guesses_log10: 2.9999999999999996

1:
  pattern: dictionary
  i: 3
  j: 6
  token: 1071
  matched_word: 1701
  rank: 1431
  dictionary_name: passwords
  reversed: true
  l33t: false
  base_guesses: 1431
  uppercase_variations: 1
  l33t_variations: 1
  guesses: 2862
  guesses_log10: 3.4566696294237573
```

How Secure Is My Password?

The #1 Password Strength Tool. Trusted and used by millions.

●●●●●●●

It would take a computer about

1 second

to crack your password

Test Your Password		Minimum Requirements
Password:	ncc1071	• Minimum 8 characters in length • Contains 3/4 of the following items: - Uppercase Letters - Lowercase Letters - Numbers - Symbols
Hide:		
Score:	46%	
Complexity:	Good	

Additions		Type	Rate	Count	Bonus
✗	Number of Characters	Flat	*+(n*4)*	7	+ 28
✗	Uppercase Letters	Cond/Incr	*+((len-n)*2)*	0	0
✓	Lowercase Letters	Cond/Incr	*+((len-n)*2)*	3	+ 8
✓	Numbers	Cond	*+(n*4)*	4	+ 16
✗	Symbols	Flat	*+(n*6)*	0	0
✓	Middle Numbers or Symbols	Flat	*+(n*2)*	3	+ 6
✗	Requirements	Flat	*+(n*2)*	2	0
Deductions					
✓	Letters Only	Flat	*-n*	0	0
✓	Numbers Only	Flat	*-n*	0	0
!	Repeat Characters (Case Insensitive)	Comp	-	4	- 2
✓	Consecutive Uppercase Letters	Flat	*-(n*2)*	0	0
!	Consecutive Lowercase Letters	Flat	*-(n*2)*	2	- 4
!	Consecutive Numbers	Flat	*-(n*2)*	3	- 6
✓	Sequential Letters (3+)	Flat	*-(n*3)*	0	0
✓	Sequential Numbers (3+)	Flat	*-(n*3)*	0	0
✓	Sequential Symbols (3+)	Flat	*-(n*3)*	0	0

Legend

✓ **Exceptional:** Exceeds minimum standards. Additional bonuses are applied.
✓ **Sufficient:** Meets minimum standards. Additional bonuses are applied.
! **Warning:** Advisory against employing bad practices. Overall score is reduced.
✗ **Failure:** Does not meet the minimum standards. Overall score is reduced.

Password: !@#$%^&*

The test

Password to test: !@#$%^&* Break it down!

```
Estimating strength of password "!@#$%^&*" ...

Average number of guesses needed to crack: 6049.000000000001
Strength score (1-5): 2
WARNING: Straight rows of keys are easy to guess
Suggestion 1: Add another word or two. Uncommon words are better.
Suggestion 2: Use a longer keyboard pattern with more turns

Approx times to crack ...
   100/hour: 3 days
  10/second: 10 minutes
 10k/second: less than a second
 10B/second: less than a second
```

```
How the password "!@#$%^&*" was broken into parts:

0:
  pattern: spatial
  i: 0
  j: 7
  token: !@#$%^&*
  graph: qwerty
  turns: 1
  shifted_count: 8
  guesses: 6048.000000000001
  guesses_log10: 3.78161178249315
```

How Secure Is My Password?

The #1 Password Strength Tool. Trusted and used by millions.

••••••••

It would take a computer about

64 milliseconds

to crack your password

Test Your Password		Minimum Requirements
Password:	!@#$%^&*	• Minimum 8 characters in length • Contains 3/4 of the following items: - Uppercase Letters - Lowercase Letters - Numbers - Symbols
Hide:		
Score:	74%	
Complexity:	Strong	

Additions		Type	Rate	Count	Bonus
✓	Number of Characters	Flat	+(n*4)	8	+ 32
✗	Uppercase Letters	Cond/Incr	+((len-n)*2)	0	0
✗	Lowercase Letters	Cond/Incr	+((len-n)*2)	0	0
✗	Numbers	Cond	+(n*4)	0	0
✓	Symbols	Flat	+(n*6)	8	+ 48
✓	Middle Numbers or Symbols	Flat	+(n*2)	6	+ 12
✗	Requirements	Flat	+(n*2)	2	0
Deductions					
✓	Letters Only	Flat	-n	0	0
✓	Numbers Only	Flat	-n	0	0
✓	Repeat Characters (Case Insensitive)	Comp	-	0	0
✓	Consecutive Uppercase Letters	Flat	-(n*2)	0	0
✓	Consecutive Lowercase Letters	Flat	-(n*2)	0	0
✓	Consecutive Numbers	Flat	-(n*2)	0	0
✓	Sequential Letters (3+)	Flat	-(n*3)	0	0
✓	Sequential Numbers (3+)	Flat	-(n*3)	0	0
!	Sequential Symbols (3+)	Flat	-(n*3)	6	- 18

Legend

- **Exceptional:** Exceeds minimum standards. Additional bonuses are applied.
- **Sufficient:** Meets minimum standards. Additional bonuses are applied.
- **Warning:** Advisory against employing bad practices. Overall score is reduced.
- **Failure:** Does not meet the minimum standards. Overall score is reduced.

Password: understandingbydivisionspite

The test

Password to test: understandingbydivision Break it down!

```
Estimating strength of password "understandingbydivisionspite" ...

Average number of guesses needed to crack: 1696241920000
Strength score (1-5): 5

Approx times to crack ...
   100/hour: centuries
  10/second: centuries
 10k/second: 5 years
 10B/second: 3 minutes
```

How the password **"understandingbydivisionspite"** was broken into parts:

```
0:
  pattern: dictionary
  i: 0
  j: 12
  token: understanding
  matched_word: understanding
  rank: 1244
  dictionary_name: us_tv_and_film
  reversed: false
  l33t: false
  base_guesses: 1244
  uppercase_variations: 1
  l33t_variations: 1
  guesses: 1244
  guesses_log10: 3.0948203803547996

1:
  pattern: dictionary
  i: 13
  j: 14
  token: by
  matched_word: by
  rank: 11
  dictionary_name: english_wikipedia
  reversed: false
  l33t: false
  base_guesses: 11
  uppercase_variations: 1
  l33t_variations: 1
  guesses: 50
  guesses_log10: 1.6989700043360185

2:
  pattern: dictionary
  i: 15
  j: 22
  token: division
  matched_word: division
  rank: 220
  dictionary_name: english_wikipedia
  reversed: false
  l33t: false
  base_guesses: 220
  uppercase_variations: 1
  l33t_variations: 1
  guesses: 220
  guesses_log10: 2.342422680822206

3:
  pattern: dictionary
  i: 23
  j: 27
  token: spite
  matched_word: spite
  rank: 2120
  dictionary_name: us_tv_and_film
  reversed: false
  l33t: false
  base_guesses: 2120
  uppercase_variations: 1
  l33t_variations: 1
  guesses: 2120
  guesses_log10: 3.326335860928751
```

How Secure Is My Password?

The #1 Password Strength Tool. Trusted and used by millions.

••••••••••••••••••••••••••••

It would take a computer about

3 sextillion years

to crack your password

Test Your Password		Minimum Requirements
Password:	tandingbydivisionspite	• Minimum 8 characters in length • Contains 3/4 of the following items: - Uppercase Letters - Lowercase Letters - Numbers - Symbols
Hide:	☐	
Score:	26%	
Complexity:	Weak	

Additions		Type	Rate	Count	Bonus
✓	Number of Characters	Flat	+(n*4)	28	+ 112
✗	Uppercase Letters	Cond/Incr	+((len-n)*2)	0	0
✓	Lowercase Letters	Cond/Incr	+((len-n)*2)	28	0
✗	Numbers	Cond	+(n*4)	0	0
✗	Symbols	Flat	+(n*6)	0	0
✗	Middle Numbers or Symbols	Flat	+(n*2)	0	0
✗	Requirements	Flat	+(n*2)	2	0
Deductions					
!	Letters Only	Flat	-n	28	- 28
✓	Numbers Only	Flat	-n	0	0
!	Repeat Characters (Case Insensitive)	Comp	-	19	- 1
✓	Consecutive Uppercase Letters	Flat	-(n*2)	0	0
!	Consecutive Lowercase Letters	Flat	-(n*2)	27	- 54
✓	Consecutive Numbers	Flat	-(n*2)	0	0
!	Sequential Letters (3+)	Flat	-(n*3)	1	- 3
✓	Sequential Numbers (3+)	Flat	-(n*3)	0	0
✓	Sequential Symbols (3+)	Flat	-(n*3)	0	0

Legend

✓ **Exceptional:** Exceeds minimum standards. Additional bonuses are applied.
✓ **Sufficient:** Meets minimum standards. Additional bonuses are applied.
! **Warning:** Advisory against employing bad practices. Overall score is reduced.
✗ **Failure:** Does not meet the minimum standards. Overall score is reduced.

Strength Scores
Following the format of each website:
Password Strength Checker -> How secure is my password -> Password Meter

123456: 1 -> Instant Brute Force -> 4%
qwerty123: 1 -> Instant Brute Force -> 41%
ncc1071: 3 -> 1 second Brute Force -> 46%
!@#$%^&*: 2 -> 64 millisecond Brute Force -> 74%
understandingbydivisionspite: 5 -> 3 sextillion year Brute Force -> 26%

1b.

Password Strength Checker said the strongest password was **understandingbydivisionspite**

How Secure Is My Password said the strongest password was **understandingbydivisionspite**

Password Meter said the strongest password was !@#$%^&*

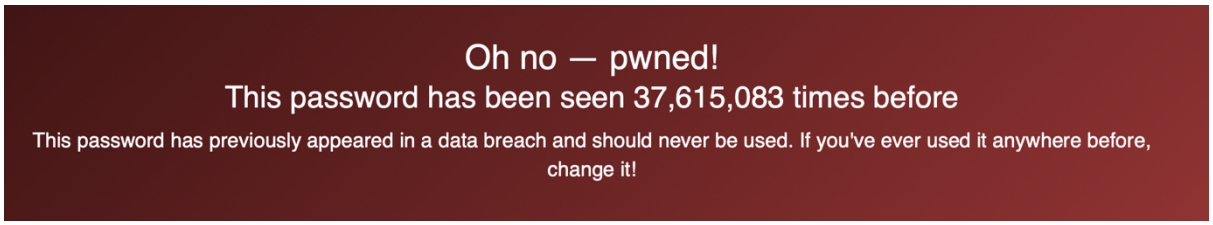
The length of understandingbydivisionspite made it the strongest password according to the first two checkers. This is interesting as there are no symbols, numbers and uppercase at any point in the password. Password Meter however thought !@#$%^&* was the strongest password even though the password is able to be typed out over one line on the keyboard. It was considered very weak by the other two password checkers as it had no letters or numbers – just symbols (one key after the other).

If you consider the requirements for each password checker some clearly valued the length of the password in regards to uppercase, numbers or symbols. This means that maybe a longer password reaching up to 26 characters long without numbers or symbols might be better than a shorter password with just letters and numbers. Each of these passwords checked was obviously missing something, it that were to be symbols, numbers, uppercase letters, straight-line of keys (e.g. 123456) or the length being at least 8 characters long. Something can clearly be added to each of the passwords tested, even for the easy ones, to make these passwords much stronger, for example: Qw3rTy123 or NcC1O71.

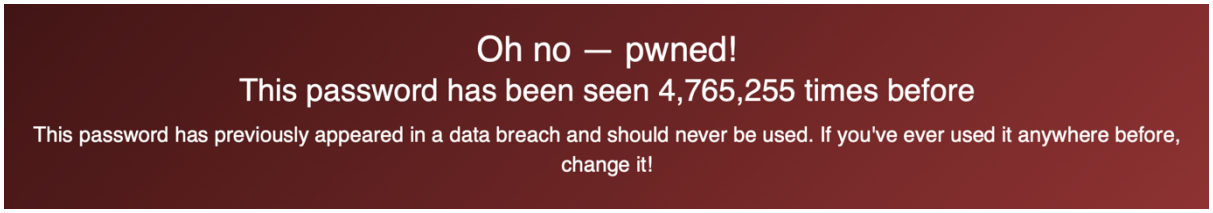
1c.

https://haveibeenpwned.com/Passwords.

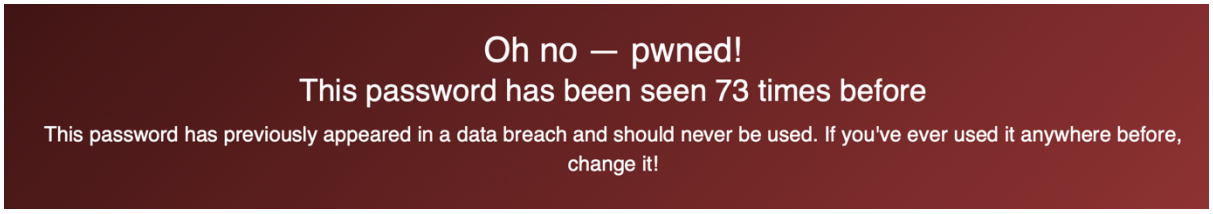
Password: 123456



Password: qwerty123



Password: ncc1071



Password: !@#$%^&*

Password: understandingbydivisionspite

1d.

Before using the 'have I been pwned' website I would have used 'ncc1071' due to the fact that it followed most of the recommendations for a strong password, e.g. both uses letters and numbers, none of the letters in a straight line on the keyboard. This would've been a useful password to adapt to stop an attacker from getting it as it is missing only; length, symbols, uppercase letter, repeated letters (cc). However based on the 'have I been pwned' website it clearly has shown that the password most likely to minimise the change of an attacker either brute-forcing or guessing is the password 'understandingbydivisionspite'.

This passwords main attribute is just its length and randomness or letters even though it is four words, it has no numbers, uppercase letters, or symbols. After doing a 'pwned' check, every password apart from 'understandingbydivision' appeared in the data breach and had been seen many times. The second lowest is the password 'ncc1071' which had been seen only 73 times which is very low compared to other passwords such as 'querty123' which is also a password using lowercase letters and numbers which had been seen a total of 4,765,255 times.

This shows that length is a defining factor on having a strong password, therefore 'understandingbydivisionspite' is a password that would be my pick in minimising the chance of an attacker either brute-forcing it or attacking it.

1e.

If a website records a password, the chances are is that it would/could end up in a data breach which would mean my personal information as well as accounts would therefore be vulnerable to be accessed by a hacker attacking them.

Websites like 'Have I Been Pwned' and 'Password strength checker' are a HTTPS website. They use a SSL security certificate to encrypt information between both its visitors and website. This would therefore mean that any information entered on these websites is unable to be intercepted by a 'cyber attacker' and processed securely. 'Password strength Checker' also uses JavaScript to check passwords. This does not require web connection after the page has loaded as it never sends the passwords to the founder webserver (Ben). Cool stuff man very cool.

Have I been Pwned also uses k-anonymity which is a mathematical concept that is widely employed in various fields. This allows the release of anonymous yet useful datasets by implementing range queries on password hashes. By using this technique, the website never acquires enough information about non-breached password hashes to compromise their security at a later time, therefore ensuring an enhanced protection for a website users password as well as maintaining their confidentiality.

This shows that both of these websites have got an effective strategy to minimise the risk of their users password being recorded.

2a.

A vishing attack would be carried out by someone to obtain sensitive personal information from the victim. The information gathered by an attack like this is generally for the attackers own gain in most cases for financial benefit. An example of a vishing attack would be targeting a victims financial credentials.

2b.

The repercussions of falling victim to vishing, or voice phishing, can be distressing. Unauthorized access to credit card and financial details can occur, resulting in the draining of the victims bank accounts. Additionally, the trust and confidence that the victim had in the company associated with the attacker may be shattered, leading them to server ties with the company. It is important to note that despite the attacker having zero affiliation with a company, the use of a spoofed caller ID can deceive the victim into believing their claims, for example: impersonating an internet/phone provider.

2c.

By exploiting a Verizon's customer service support line this lead the attacker to obtain the victims email. Subsequently they proceeded to create another account they could access within the victims existing account and, effectively removing the victim by changing the password. This resulted in the attacker having complete control over the victims Verizon account enabling them to access private and personal data and information that was stored within it.

2d.

Employing social engineering techniques and a spoofing tool, the hacker manipulated the caller ID to appear as though she was dialling from the 'victims' own number on her personal device. To solidify her ruse as a concerned mother in need of assistance, she then skilfully used distraction tactics which included playing a video which had a baby crying in the background of her end of the call. This combination allowed her to gain deception to then exploit the man's empathy, on the other end, as well as his willingness to offer help.

2e.

The hacker possessed exceptional interpersonal skills which allowed her to engage with the Verizon customer service representative in a 'relatable' manner, in this case to women in particular mothers with children. Her speech as well as the urgency she conveyed were attributed to her child's needs rather than an her actual motive of scamming her victim. Her voice had modulation as well as a pleasant vibrato which allowed her to present herself as a trustworthy individual to converse with, effectively appearing non-threatening in the process.

2f.

The attacker induced a heightened sense of urgency within the company by assuming the persona of a distressed mother caring for a young child. To enhance the illusion she played baby noises in the background, accompanied by visible signs of stress and distraction. The combination of this as well as distracting elements led to the success lent credibility of the attackers narrative effectively deceiving the customer support rep who handled the call. By presenting themselves as a relatable person this resulted in the attacker avoiding suspicion in particular when she said "Will you help me?" stressfully during an explanation of her situation.

2g.

By exploiting the gendered stereotype of a absent husband while caring for their baby, she gained and leveraged this perception to enhance the credibility for her to 'resolve' their Verizon accounts. By portraying herself as a panicked individual as well as juggling the demands of a crying baby while stressing over phone provider accounts created an atmosphere that was genuine and relatable. Through exploiting this social norm and stereotype it added authenticity, legitimacy increasing the likelihood of her depiction.

2h.

A security measure that would've prevented this have from being a success is Two-Factor Authentication(2FA). With 2FA you would need a password (Single-Factor Authentication) as well as something else before you are able to log in.

The 'something else' can classify it to be something you know, something you have, something you are. Examples of 'something you know' could be; a PIN number, your place of birth, a Passphrase, childhood pet

name. Examples of 'something you have' could be; a software that would send a notification to your phone or tablet that would provide you with an access code, your phone getting a call. Examples of 'something you are' could be; a voice recognition, fingerprint scans, faceID.

I would advise the victim to enable 2FA with Verizon as well as their other accounts. This additional security measure would typically involve security questions that would require personal knowledge, such as "Where did you grow up?" or "What was the name of your high school?". Setting up 2FA using these questions provides an additional level of security for accessing or making changes to personal information.

To prevent falling victim to similar scams in the future, the victim should educate themselves about these types of hacks as it is crucial to be aware that legitimate companies would never initiate contact via phone calls or text messages to request personal information. Any sense of urgency or requests for personal information from such callers are red flags indicating a likely scam. It is important to remember that trained customer service representatives would not rush or pressure individuals when asking for information.

By staying informed and cautious, the victim can proactively safeguard themselves against scams and protect their personal information.

2i.

Verizon should prioritize the implementation of two-factor authentication for their clients, providing an additional layer of security. Furthermore, they should enhance their verification process by requiring additional questions or information when handling requests to modify account details on behalf of others. It is crucial for Verizon to invest in comprehensive training programs for their customer support agents to effectively recognize and respond to scamming attacks. Failing to do so could lead to customer dissatisfaction, potential customer loss, and subsequent revenue decline. By actively addressing these security concerns, Verizon can reinforce customer trust, safeguard their accounts, and maintain a strong customer base.

3a.

Username: anonymous
Password: ian.welch@vuw.ac.nz

3b.

rainmaker.wunderground.com

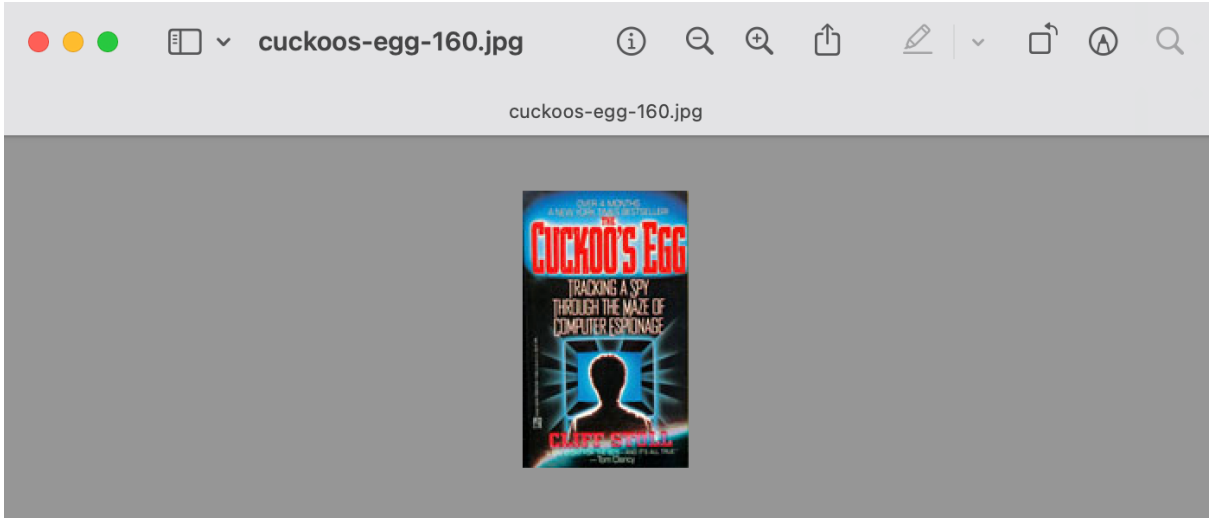
3c.

Address associated with the user's computer is: (20:16:b9:f9:1f:dc)

3d.

www.columbia.edu

3e.



4a.

According to the article, the fraudsters employed many steps to make the advertisements seem legitimate to potential buyers. Here is some of the steps they took:

- Correspondence with Victim Buyers: They employed people to then go on to correspond with the people who fell for the listings by email and sent fake ownership papers to create a believable and compelling story for buyers to part with their money.
- Saturation of Internet Marketplace Websites: They flooded many popular marketplace websites (eBay, Cars.com, AutoTrader.com) with extensive listings for cars, boats as well as other expensive items all ranging between $10,000 - $45,000.
- Exploitation of Emotional Appeals: The fraudsters created websites for their fake car dealerships where they created stories as to why they were selling such items. One fraudster, by the name of Ghebosila, who was posing as widow of an Iraq war vet who was selling her families mobile home so she could afford to take care of her children.
- Counterfeit Payment Services: To facilitate transactions, the fraudsters created counterfeit invoices pretending to be from Amazon Payments and PayPal. After the fraudster came to an agreement with the victim, they gave them electronic payment instructions. They used branding in the fake invoices so that they would be identical to the online payment services they were pretending to be from so it would be believable to the victim. The invoices directed the victims to send their money to American Bank Accounts owned by “Arrows” where it was then being sent to the fraudsters.
- Use of “Arrows” and Fake Passports: The fraudsters had co-conspirators, referred to as “arrows”, who used fake passports to open bank accounts in the United States. These accounts were used to receive funds from victims who fell into these scams.
- Money Laundering and Concealment: They fraudsters used various methods to launder the fraudulent proceeds. Examples of this included concealing cash inside audio speakers as well as using the funds to purchase expensive and luxury items to be sold off back in Europe.

By executing these steps, the fraudsters aimed to create an illusion of legitimacy, manipulate emotions and exploit trust to defraud unsuspecting buyers on online marketplaces.

4b.

The affect heuristic is a cognitive shortcut that plays a significant role in decision-making processes. It involves individuals making swift and efficient judgments based primarily on their current emotional state, rather than relying on factual or concrete information. This heuristic allows people to simplify complex situations by relying on their emotional reactions as a guide.

Pretexting is a form of social engineering used by attackers to manipulate and deceive victims. In pretexting, the attacker creates a fabricated story or scenario to gain the trust and cooperation of the victim. By employing persuasive storytelling techniques, the attacker aims to convince the victim to provide valuable information that can be exploited for immoral purposes.

Both the affect heuristic and pretexting highlight the influence of emotions and psychological manipulation in decision-making and social engineering tactics, respectively. Understanding these concepts can help individuals become more aware of the potential biases and vulnerabilities that can be exploited in various situations.

4c.

- Verify the authenticity of the website: Pay attention to the websites appearance and professionalism. Look out for signs of poor spelling, grammar, or a suspicious URL, as these could indicate a fraudulent website. Check if the website provides comprehensive contact details and information. Legitimate websites usually have clear ways to reach out to them. Look for customer reviews on the website. Ensure that the reviews are varied in content and come from different individuals, as this adds credibility.
- Use Trusted Payment Systems: Avoid using email as a payment method altogether. Instead, opt for secure payment systems like PayPal. Legitimate payment systems would not ask for payment details via email or send invoices with bank transfer information. Using trusted payment platforms adds an extra layer of protection, as they often have built-in fraud prevention measures and dispute resolution processes.
- Be Cautious of unrealistic deals: If a deal seems too good to be true, exercise caution. Especially when purchasing expensive items like boats or cars, be skeptical of sellers who refuse in-person meetings or test drives. Ensure that the seller provides sufficient information and a valid address for inspection purposes. If possible, arrange a face-to-face meeting to verify the items condition and legitimacy.
- Watch Out for Suspicious Offers and Urgency: Any internet shopping websites or online listings that promises excessive benefits without providing proper details and at an unusually low price should raise suspicions. Beware of sellers who create a sense of urgency, pressuring you to make a quick decision. Take your time to evaluate the offer and do thorough research before committing to a purchase.
- Use Reputable Resale Websites with Buyer Protections: When buying from resale websites, choose platforms that have established seller protections in place. These websites often act as intermediaries, holding the funs until the buyer confirms receipt of the item. Familiarize yourself with the specific buyer protections offered by the website and review them carefully before making any purchases.
- Request Evidence and Documentation: Ask the seller to provide photos of the product, preferably with something that proves the pictures were taken recently. For valuable or specialized items like antiques, luxury goods, or expensive electronics, request certificates of authenticity, serial/model numbers, and additional pictures of labels or stitching.
- Ensure Website Security: Before entering any personal or financial information, check if the website has a secure connection. Look for a padlock symbol in the URL bar, indicating that the website is encrypted with HTTPS SSL certificate. An encrypted connection prevents unauthorized access to your sensitive data, such as credit card details, ensuring a higher level of security.
- Avoid Upfront Payments for High-Value Items: Never pay the full amount upfront for costly items like cars without seeing them in person. Legitimate sellers often require a deposit, with the balance payable upon receipt or through an agreed payment plan. Beware of sellers who insist on immediate full payment before any physical inspection. Such demands are often red flags for potential fraud.
- Ensure Website Security: Before entering any personal or financial information, check if the website has a secure connection. Look for a padlock symbol in the URL bar, indicating that the website is encrypted with HTTPS SSL certificate. An encrypted connection prevents unauthorized access to your sensitive data, such as credit card details, ensuring a higher level of security.

By following these precautions, you can significantly reduce the risk of falling victim to online fraud when purchasing expensive items. Remember to prioritize your safety and take the necessary steps to verify the authenticity of both the seller and the website before making any financial commitments.

5.a

Home Repair Con: A contractor comes to your home claiming that they are doing free inspections and estimates for home repairs. They will find something alarming wrong and offer to fix it for a reasonable price, and the home owner agrees because they are worried about their home. The "contractor" takes a deposit, and never comes back – Wikipedia("List of Confidence Tricks").

Home improvement scams often prey on homeowners by employing various manipulative tactics. Scammers may request upfront payment or a deposit, only to disappear without completing the work. Alternatively, they may perform substandard work or claim to have discovered additional issues that require immediate attention, thereby inflating the cost of repairs. These scams take advantage of homeowners vulnerability, particularly those with limited knowledge of home repairs and improvements. These fraudulent schemes exploit basic human desires and cognitive biases to elicit intuitive reactions and discourage victims from recognising the scam.

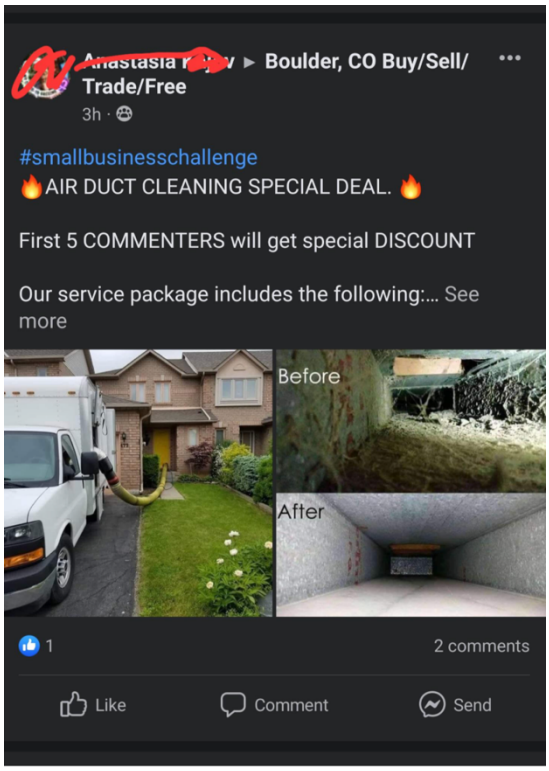
The affect heuristic plays a role in this, as individuals tend to base their judgments on the perceived character of a person rather than considering the social and environmental factors influencing their actions. Additionally, the "Just World Hypothesis" leads initials to believe that good deeds result in positive outcomes, creating a mental assumption that they will be rewarded for their actions. This belief in a just world helps scammers overcome obstacles and rationalize their actions, as they exploit victim's trust.

Several principles from Cialdini's Principles of Influence are often at play in these scams:

- Reciprocity: People feel obligated to reciprocate when they receive something from others. If scammers offer free inspections or quote home repairs, victims may feel obliged to repay their kindness, even if the intention is to deceive and extract money. The promise of a special deal or discounted rate can also evoke a sense of reciprocity, even though the scammer's objective is to exploit the homeowner.
- Consistency (Commitment): Once individuals make a choice, they tend to stick with it. After selecting a builder or home maintenance company and paying a deposit, victims are less likely to switch companies, even if warning signs arise.
- Social Proof: People tend to trust and follow the actions of others. Scammers may create fake social media profiles and reviews, showcasing images and testimonials that resemble the victim's lifestyle. This tactic aims to create familiarity and credibility, increasing the chances of successful deception. Additionally, if the scammer can enlist individuals with similar demographics to the victim to discuss supposed work done on their properties in videos, it further strengthens the illusion of legitimacy.
- Liking: People are more inclined to comply with requests from individuals they like. Scammers often employ tactics to appear amiable, such as offering compliments on the homeowner's property and establishing common goals for improvement. They may even establish associations with reputable building or tool suppliers to enhance their likeability and perceived authority.
- Authority: People tend to follow individuals who appear knowledgeable and authoritative. Scammers may present themselves as reputable maintenance or repairs professionals, displaying expertise in their field to gain trust.
- Scarcity: People are drawn to exclusive opportunities or limited resources. Scammers exploit this by offering "special deals" available only for a limited time, creating a sense of urgency and desire to obtain the offer. This tactic taps into the concept of "Phantom Fixation", where individuals become so captivated by an alluring prize or reward that they abandon their own judgment in pursuit of it.

It is crucial for homeowners to be aware of these tactics and exercise caution when engaging with contractors or service providers. Conduct thorough research, seek multiple opinions, and never make upfront payments without verifying the legitimacy and credibility of the individuals or companies involved.

5b.



In the digital adaptation of this scam, scammers would leverage various online resources to target individuals with enticing home improvement opportunities. They would utilize social media platforms to advertise their services, strategically placing ads that catch the attention of potential victims. These ads would be carefully designed to create associations between the idea of home improvement and the fraudulent company, using colors, shapes, and persuasive language to subtly influence viewers.

To enhance credibility and exploit the Social Proof Principle, the scammers would employ tactics such as hacking into individual's social media accounts (Facebook) and sending messages to their friends. These messages would boast about recent home maintenance projects such as fence installations, chimney cleaning, etc. This was carried out to spark curiosity and inquiries about the company responsible for the work. Once friends' express interest, the scammers would provide contact information for the fraudulent company and insist on receiving a deposit before any work can be scheduled.

By using a victim's own friends as unwitting endorsers, the scammers aim to create a sense of trust and legitimacy. Victims, influenced by the Social Proof Principle, would be more inclined to believe the scam and proceed with paying the deposit. The scammers would craft the digital ads and messages with meticulous attention to detail, ensuring they appear professional and legitimate, free of any grammatical errors. Urgency and special deals would also be incorporated into the ads to create a sense of immediacy and entice victims to act quickly.

Unlike the traditional scam where scammers choose specific aspects of a victim's house to work on, the digital version would offer a range of project options. This approach increases the scams efficiency and effectiveness online. The scammers would present different deals for various home improvement projects, providing victims with the illusion of choice and customization.

Through this digital adaption, scammers exploit the power of online advertising, social connections, and the persuasive impact of targeted messaging. Victims are manipulated through social proof, subconscious engagement, and the allure of special deals. It is essential for individuals to remain vigilant and skeptical of online advertisements and unsolicited message, ensuring they thoroughly research and verify the legitimacy of any company or service before making any payments or commitments.

5c.

My scam drew inspiration from online prize and sweepstake scams, specifically those involving targeted advertisements offering a chance to win a prize in exchange for a paid ticket entry. The digital scam bears similarities to its analog counterpart, where scammers require a deposit to gain access to the supposed prize of "home improvement". Whether in person or online, the scammer focuses on building targeted trust. In the online version, this is achieved through precisely tailored advertisements that cater to the users' interests. These ads are designed to captivate the user's attention and entice them to participate in the prize draw.

In the analog version, trust is established through personal interactions. The scammer showcases example pictures of their purported home improvement projects, creating an illusion of credibility and expertise. By presenting visual evidence of their past work and highlighting potential improvements for the user's own home, they effectively persuade victims to believe in the scam.

Both versions of the scam leverage targeted approaches to manipulate victims. In the digital realm, target ads are deployed to engage users on a subconscious level, tapping into their interests and desires. This tailored approach is aimed at creating a strong association between the idea of winning a prize and the scammers fraudulent operation.

Similarly, in the analog version, scammers use personalized interactions to forget a connection with the victim. By showcasing visuals and discussing potential improvements, they play on the victim's desire for an enhanced home and exploit the trust that is built during these interactions.

It is crucial for individuals to remain cautious and skeptical when encountering such prize-based scams, whether online or offline. Verifying the legitimacy of the offer, conducting thorough research on the organization or individual behind the scheme, and avoiding making any payments or providing personal information upfront are essential steps to protect oneself from falling victim to these manipulative tactics.

5d.

To transition this home improvement scam into the digital age, several changes and additions are necessary. Firstly, the scam would no longer rely on face-to-face interactions. Instead, it would be conducted entirely through digital platforms, allowing the fraudster to operate from anywhere in the world, making the scam more scalable and efficient.

One crucial aspect for the digital version of the scam would be establishing an online presence for the company. This involves creating and maintaining active social media accounts, particularly on platforms such as Facebook. The fraudster would need to invest in developing Facebook ad skills and copywriting to effectively target and engage potential victims online. If they lack these skills, they may need to hire someone with expertise in digital marketing to assist them in crafting persuasive ads and maintaining a strong online company image.

However, finding someone willing to participate in this scam, even with significant financial incentives, could pose a challenge. The illegal nature of the activity and the potential legal consequences may deter individuals from getting involved. Therefore, the fraudster would need to carefully navigate these challenges to ensure the success of their digital scam.

In summary, for this home improvement scam to thrive in the digital age, it would require a shift from face-to-face interactions to online platforms. Building a robust online presence, particularly on social media, and acquiring digital marketing skills would be crucial. Nonetheless, the challenges of finding willing participants and navigating legal risks remain significant considerations.

5e.

The properties of the internet, such as instantaneous communication, significantly impact the digital version of the scam. These characteristics differentiate the digital realm from the analog world and present both advantages and challenges for the fraudsters.

One key advantage is the global reach of the Internet. Scammers can exploit the instantaneous nature of online communication to target and potentially deceive a large number of people simultaneously. They can reach individuals from different geographical locations and time zones, increasing their potential pool of victims. The ability to cast a wide net and contact numerous people within a short period can enhance the scale and efficiency of the scam compared to the analog version, where the fraudsters reach is limited by physical proximity.

However, the digital environment also presents challenges for the fraudsters. People have become more cautious and skeptical due to the prevalence of online scams and fraudulent activities. The anonymity and lack of face-to-face interaction in the digital realm can create a sense of distrust and wariness among potential victims. The instantaneous communication and global nature of the internet also expose users to a vast amount of information, including warnings and stories of scams, making them more vigilant and less likely to fall for fraudulent schemes.

Additionally, the digital version of the scam may face greater scrutiny and countermeasures. Online platforms and social media networks have implemented security measures to identify and remove fraudulent content. Users are increasingly aware of online privacy and security issues, and platforms employ algorithms and reporting mechanisms to detect and block scam-related activities.

Furthermore, the ability to research and verify information online provides individuals with tools to validate the legitimacy of offers and companies. They can read reviews, check for online communities, which an act as a deterrent for falling victim to scams.

While the instantaneous communication and global reach of the Internet do offer advantages for scammers in regards of accessing a larger audience, the inherent suspicion and cautiousness of online users, as well as the availability of information and security measures, does make it more challenging to successfully pull off the digital version of the scam compared to its analog counterpart.

5f.

The analog version of this scam is more likely to be effective due to the nature of a home improvement project requiring in-person interaction. When the victim meets the fraudster face-to-face and allows them to inspect their home, there is a higher likelihood of trust being established. The fraudster can utilize persuasive techniques, such as leveraging Cialdini's Principles of Influence, more effectively in person. Non-technical social engineering skills, like interpersonal communication and a friendly demeanor, play a significant role in building trust when interacting face-to-face. These elements are more challenging to replicate and establish online, where creating the same level of trust without a personal encounter becomes difficult. While a strong social media presence may be necessary in the online version, it does not fully compensate for the lack of direct interaction and the trust-building opportunities it provides in the analog version.

6a.

Telegram: https://www.wired.com/story/telegram-encryption-whatsapp-settings/
https://telegram.org/faq
Signal: https://en.wikipedia.org/wiki/Signal_(software)#Encryption_protocols
Snapchat: https://xperylab.medium.com/decrypting-and-extracting-juicy-data-snap-17301aa57a87

All three messaging platforms mentioned employ encryption techniques to protect user communication, but there are variations in their implementations and the level of security they provide.

Telegram: Offers encryption for data transmitted between a user's device and their servers, but end-to-end encryption is not enabled by default. To ensure end-to-end encryption, users must initiate "secret chats" where messages are encrypted on the sender's device and decrypted on the recipients device. However, this feature is only available for one-on-one conversations and not for group chats. Telegram uses 256-bit symmetric AES encryption, 2048-bit RSA encryption, and a Diffie-Hellman secure key exchange to strengthen data encryption.

Signal: Takes a comprehensive approach to encryption, employing the signal protocol for end-to-end encryption on all messages. The signal protocol incorporates the double ratchet algorithm, pre keys, and a triple Diffie-Hellman handshake. It utilizes AES-256 encryption, HMAC-SHA256 for message authentication, and Curve25519 for key exchange. Signal ensures privacy by default for all conversations and does not offer optional encryption modes.

Snapchat: Implements end-to-end encryption for snaps (photos and videos), but other forms of communication, such as text chats and group interactions, are not encrypted. Memories, which are stored on

Snapchat servers, are not encrypted unless the user saves them to “My Eyes Only” and sets a password. The password for “My Eyes Only” is a 4-digit PIN, which may not offer the same level of security as longer passwords. Snapchats encryption algorithm for snaps is not explicitly mentioned, but it is suspected to be AES-256 in CBC mode.

6b.

In the context of key management in messaging services, the Signal protocol provides a mechanism to establish trust between users. When initiating a conversation with an unknown person, the signal protocol employs a double ratchet algorithm that generates a temporary key pair for each user. These temporary keys are used in addition to the permanent keys.

The continuous changing of short-lived keys in the double ratchet algorithm ensures enhanced security and makes it extremely difficult for third parties to intercept and decrypt the messages.

By utilizing this approach, the signal protocol enables users to trust the keys used by their communication partners. Each message exchanged within the conversation has its own unique key, providing an additional layer of security. This significantly reduces the risk of illegal access to the conversation and helps found trust in the encryption process provided by the messaging service.

6c.

When it comes to verifying the absence of backdoors or trojans in messaging tools, it is essential to consider the transparency and trustworthiness of the software and its underlying code. While it can be challenging for individual users to thoroughly inspect the entire codebase of messaging tools, there are certain factors that can help determine the level of trust and code verification.

Signal is known for its commitment to security and privacy. The signal protocol is open source. This means that the code is freely available for review by anyone. This allows security experts and developers to analyze the code to identify any backdoors or potential vulnerabilities. The transparency provided by open-source projects increases the probability of addressing and detecting any security issues, creating a higher level of trust in the software.

Telegram is partially open source. While the client-side code is available for inspection, the server-side code is not. This limitation makes it difficult to verify absence of backdoors or trojans within the server infrastructure. Users must rely on the reputation and trustworthiness of Telegram as a messaging service.

Snapchat is a closed-source platform. It does not offer the same level of transparency as open-source projects. Without access to the source code, users are unable to directly verify the absence of backdoors or trojans. In this case, users must trust Snapchats security measures and reputation to ensure the integrity of their platform.

In summary, the ability to verify the absence of backdoors or trojans depends on the openness and transparency of the messaging platform. Open-source projects such as Signal deliver a higher degree of code verification, while closed-source platforms such as Snapchat require users to place trust in the reputation and security practices of the service platform.

7a.

Password for carol.asc = assignment 2
No password for libr8
Converted passwd.bf.enc to asc format.

" The *admin* loves to use easy to remember passwords and it is useful to know that the password file stores passwords as MD5 hashes.
Libr8 has encrypted the file using the Blowfish algorithm in CBC mode and the password is a commonly chosen one. Furthermore, the file was encrypted in 2018 and Libr8's favourite movie is *Mirrors*."

Used mirrors hint to find password dlanod

```
Last login: Mon May 29 12:35:42 on ttys000
ssh -t  greenthom@barretts.ecs.vuw.ac.nz -p 22 "cd \/home\/greenthom\/assignment2 && exec \$SHELL
-l"
tomgreen@Toms-MacBook-Air-3 ~ % ssh -t  greenthom@barretts.ecs.vuw.ac.nz -p 22 "cd \/home\/greenth
om\/assignment2 && exec \$SHELL -l"
greenthom@barretts.ecs.vuw.ac.nz's password:
barretts% gpg --import carol.asc
gpg: key E8B80B9A637E5A39: "Carol <carol@here.com>" not changed
gpg: key E8B80B9A637E5A39: secret key imported
gpg: Total number processed: 1
gpg:              unchanged: 1
gpg:       secret keys read: 1
gpg:  secret keys unchanged: 1
barretts% gpg --import libr8.asc
gpg: key BCCA167F55BE044D: "Libr8 <liber6@there.com>" not changed
gpg: Total number processed: 1
gpg:              unchanged: 1
barretts% gpg --decrypt password.bf.enc.asc > password.bf.enc
gpg: can't open 'password.bf.enc.asc': No such file or directory
gpg: decrypt_message failed: No such file or directory
barretts% gpg --decrypt passwd.bf.enc.asc > passwd.bf.enc
gpg: Note: secret key 9AE2A76C2C83055F expired at Thu 13 Apr 2023 20:50:35 NZST
gpg: encrypted with 3072-bit RSA key, ID 9AE2A76C2C83055F, created 2021-04-13
      "Carol <carol@here.com>"
gpg: Signature made Tue 13 Apr 2021 21:06:40 NZST
gpg:                using RSA key 75F4FC6B8794CF989C956D7EBCCA167F55BE044D
gpg:                issuer "liber6@there.com"
gpg: Good signature from "Libr8 <liber6@there.com>" [expired]
gpg: Note: This key has expired!
Primary key fingerprint: 75F4 FC6B 8794 CF98 9C95  6D7E BCCA 167F 55BE 044D
barretts% openssl enc -provider legacy -provider default -bf-cbc -pbkdf2 -d -in passwd.bf.enc
enter BF-CBC decryption password:

enter BF-CBC decryption password:
admin:NzEyNWNkODg1ZDEzOWEwZmY3Nzc0NDZiNTE4OGZmMTg=
zsh: command not found: enter
barretts%
```

7b.

Used 'dlanod' password to obtain:
enter BF-CBC decryption password:
admin:NzEyNWNkODg1ZDEzOWEwZmY3Nzc0NDZiNTE4OGZmMTg=
admin password: NzEyNWNkODg1ZDEzOWEwZmY3Nzc0NDZiNTE4OGZmMTg=

Once decrypted displayed md5 hash of admin password. Used rainbow tables to provide password. Hash converted to plaintext = password: coffee1999.
Used: https://crackstation.net