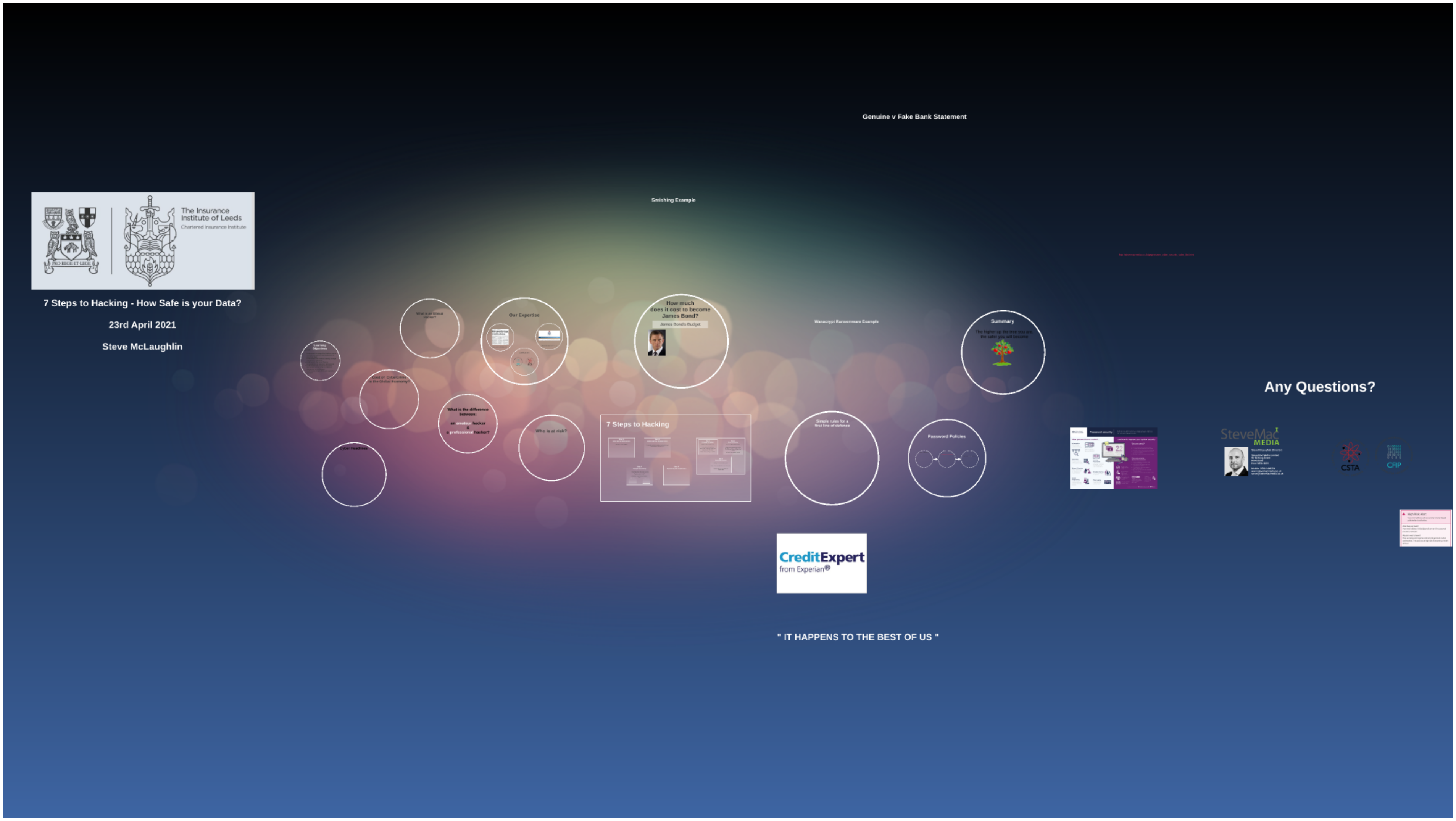


The Insurance Institute of Leeds
Chartered Insurance Institute

7 Steps to Hacking - How Safe is your Data?

23rd April 2021

Steve McLaughlin

Genuine v Fake Bank Statement

Smishing Example

Learning Objectives

What is an Ethical Hacker?

Our Expertise

How much does it cost to become James Bond?

James Bond's Budget

Cost of Cybercrime to the Global Economy?

What is the difference between:

an amateur hacker
&
a professional hacker?

Who is at risk?

Cyber Headlines

7 Steps to Hacking

Wanacrypt Ransomware Example

Summary

The higher up the tree you are the safer you will become

Simple rules for a first line of defence

Password Policies

CreditExpert from Experian®

" IT HAPPENS TO THE BEST OF US "

Any Questions?

SteveMac MEDIA

CSTA

CFIP

PRO·REGE·ET·LEGE

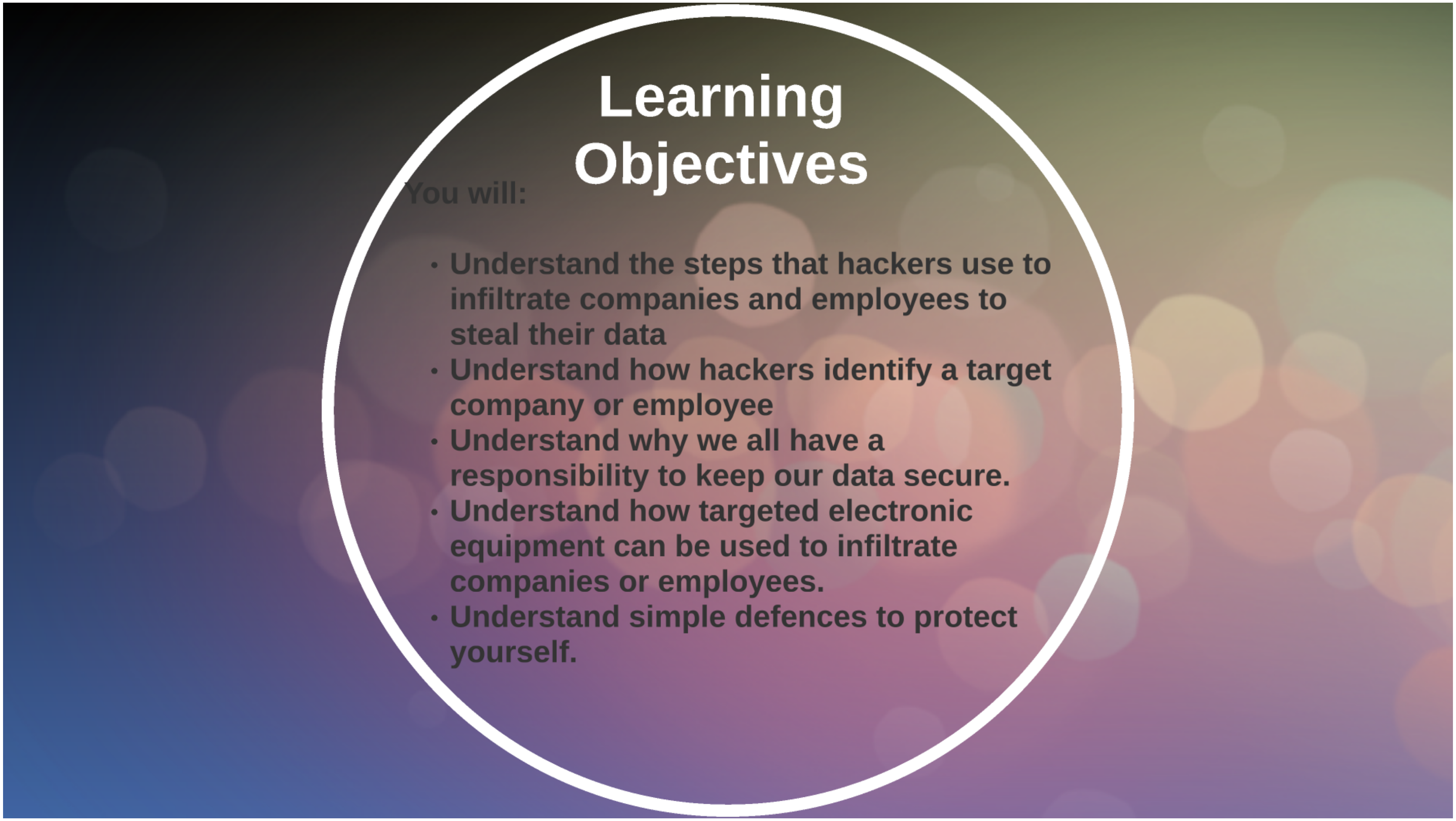
The Insurance Institute of Leeds

Chartered Insurance Institute

7 Steps to Hacking - How Safe is your Data?

23rd April 2021

Steve McLaughlin



Learning Objectives

You will:

- Understand the steps that hackers use to infiltrate companies and employees to steal their data
- Understand how hackers identify a target company or employee
- Understand why we all have a responsibility to keep our data secure.
- Understand how targeted electronic equipment can be used to infiltrate companies or employees.
- Understand simple defences to protect yourself.

Cyber Headlines

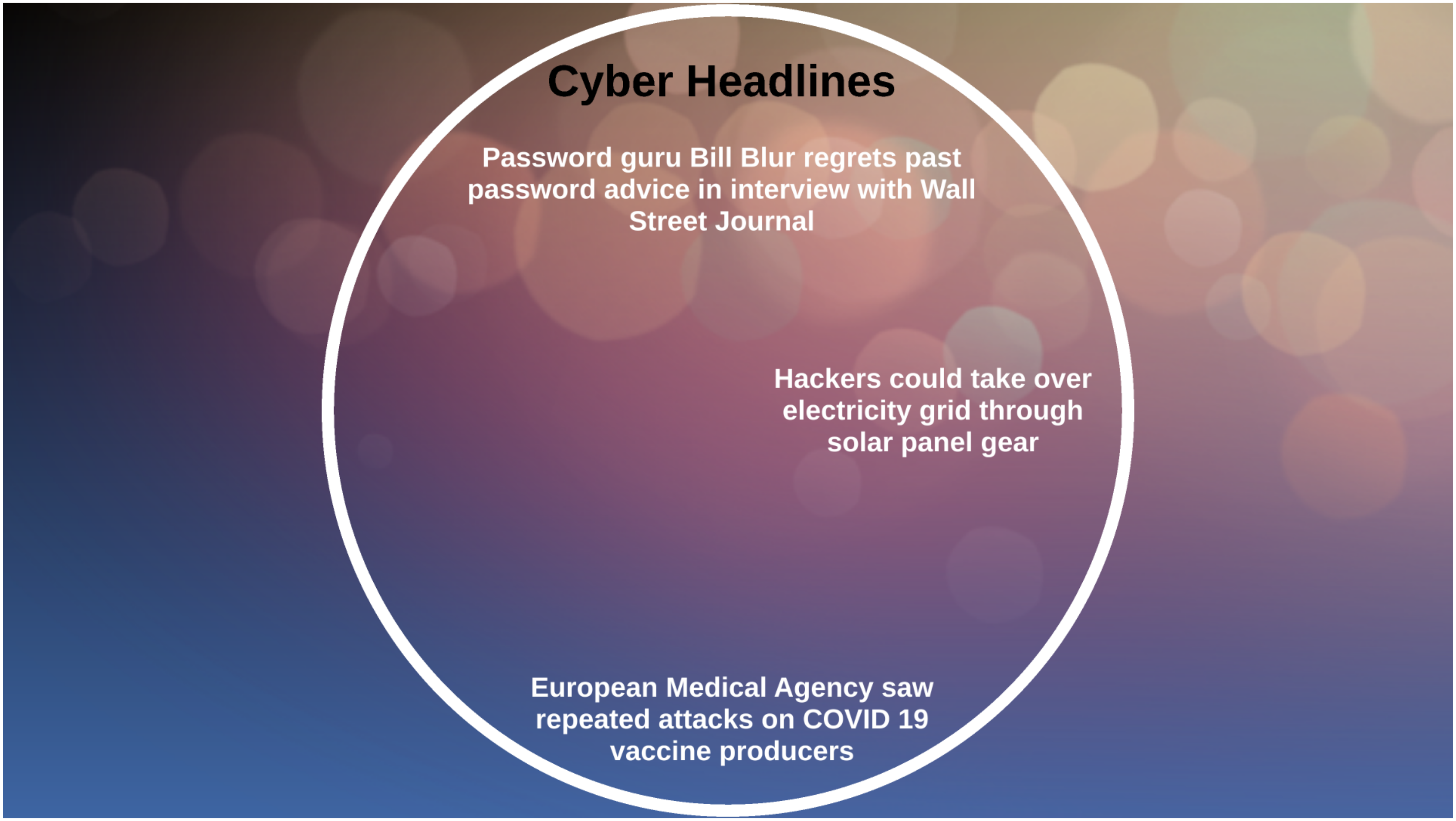
Cyber Headlines

Password guru Bill Blur regrets past password advice in interview with Wall Street Journal

Cyber Headlines

Password guru Bill Blur regrets past password advice in interview with Wall Street Journal

European Medical Agency saw repeated attacks on COVID 19 vaccine producers

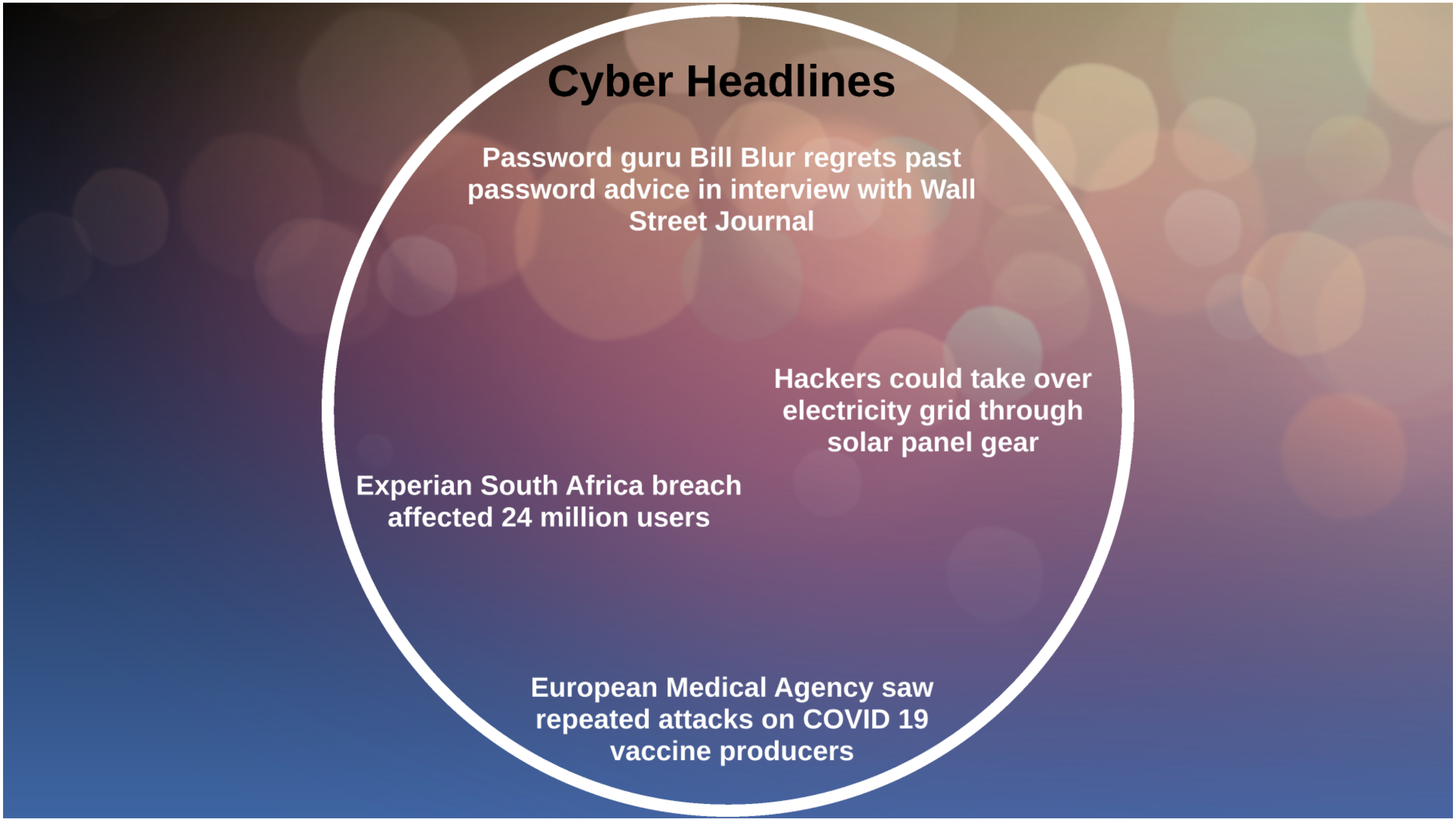


Cyber Headlines

Password guru Bill Blur regrets past password advice in interview with Wall Street Journal

Hackers could take over electricity grid through solar panel gear

European Medical Agency saw repeated attacks on COVID 19 vaccine producers



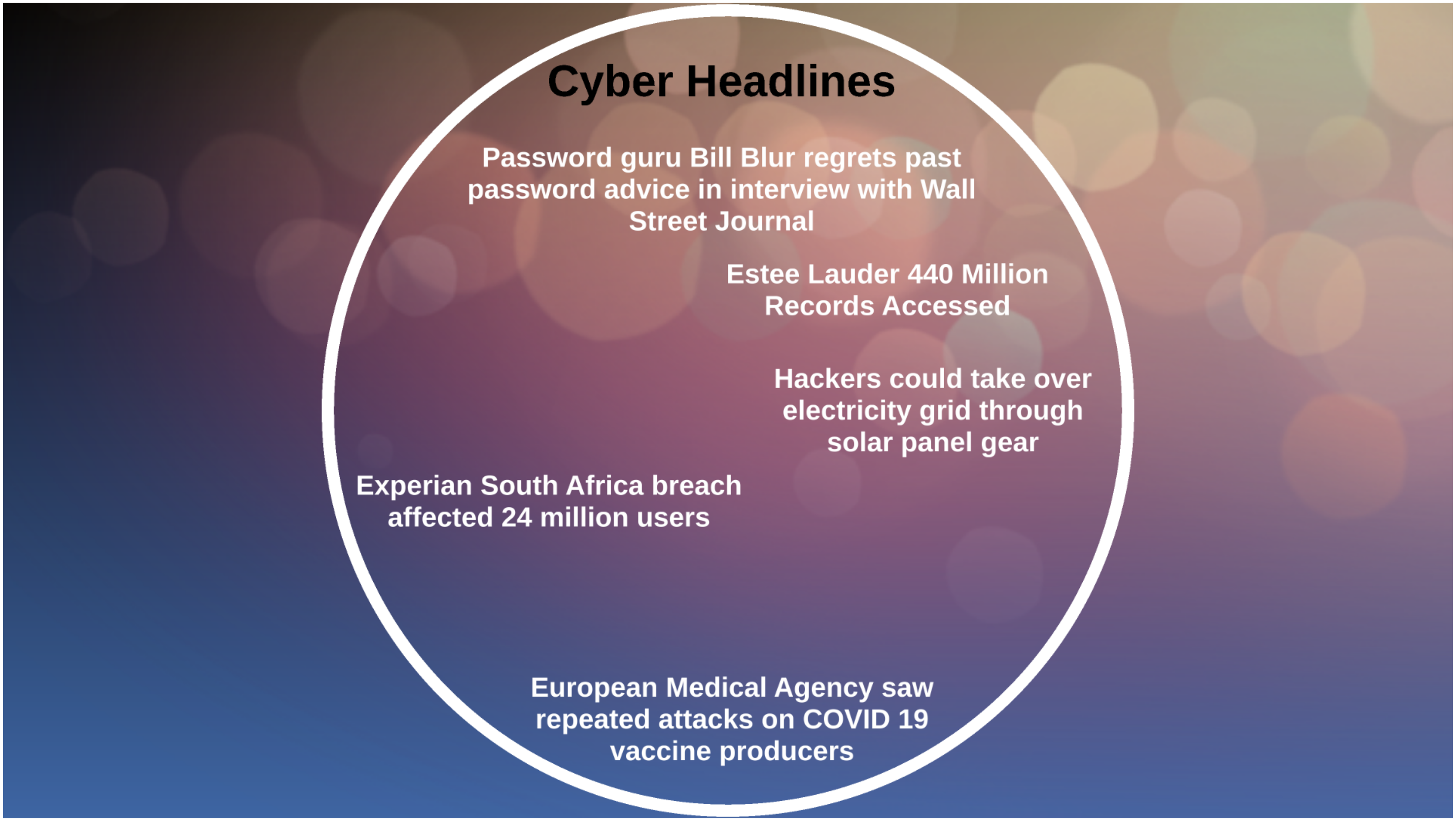
Cyber Headlines

Password guru Bill Blur regrets past password advice in interview with Wall Street Journal

Hackers could take over electricity grid through solar panel gear

Experian South Africa breach affected 24 million users

European Medical Agency saw repeated attacks on COVID 19 vaccine producers



Cyber Headlines

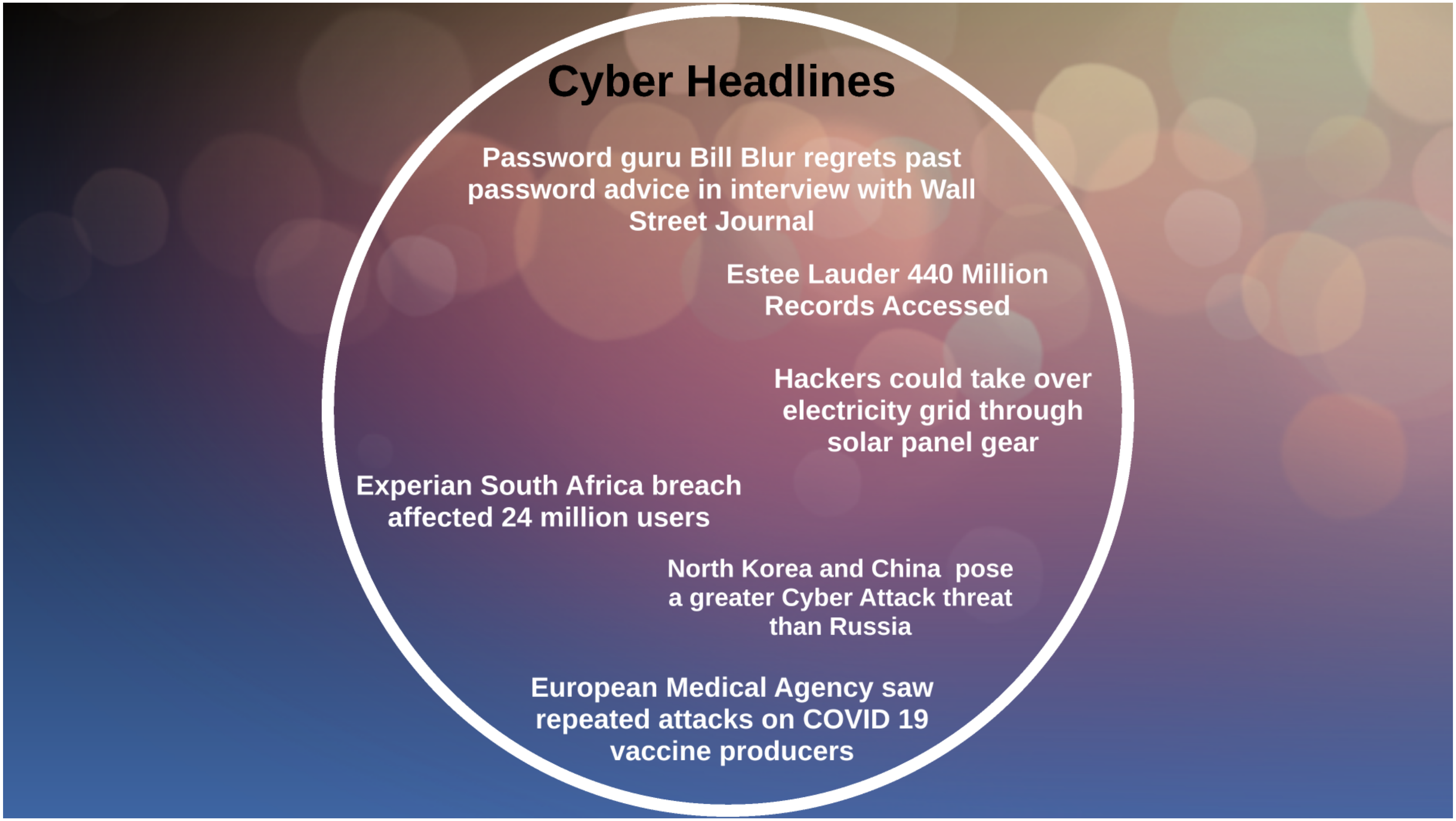
Password guru Bill Blur regrets past password advice in interview with Wall Street Journal

Estee Lauder 440 Million Records Accessed

Hackers could take over electricity grid through solar panel gear

Experian South Africa breach affected 24 million users

European Medical Agency saw repeated attacks on COVID 19 vaccine producers



Cyber Headlines

Password guru Bill Blur regrets past password advice in interview with Wall Street Journal

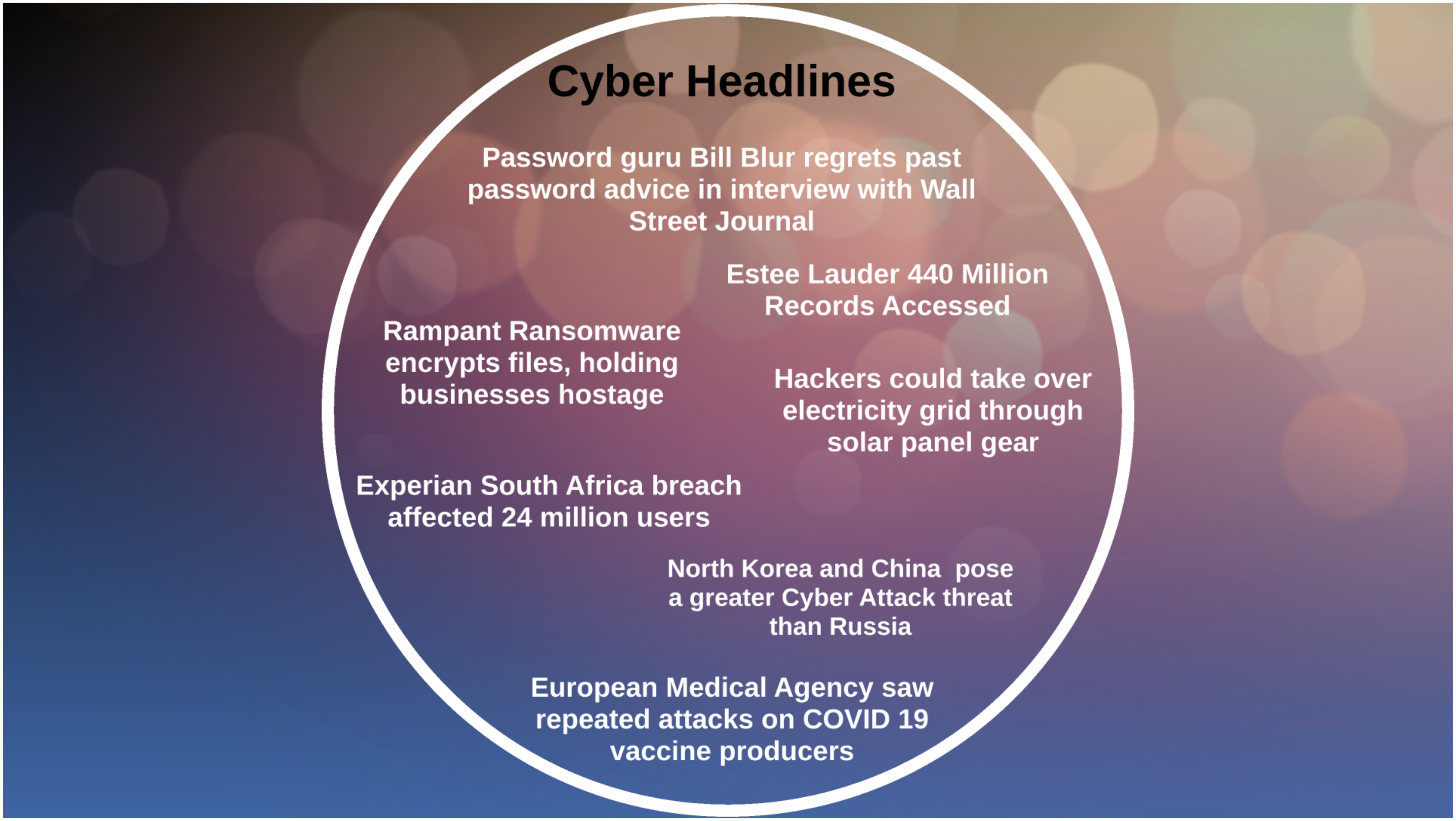
Estee Lauder 440 Million Records Accessed

Hackers could take over electricity grid through solar panel gear

Experian South Africa breach affected 24 million users

North Korea and China pose a greater Cyber Attack threat than Russia

European Medical Agency saw repeated attacks on COVID 19 vaccine producers



Cyber Headlines

Password guru Bill Blur regrets past password advice in interview with Wall Street Journal

Estee Lauder 440 Million Records Accessed

Rampant Ransomware encrypts files, holding businesses hostage

Hackers could take over electricity grid through solar panel gear

Experian South Africa breach affected 24 million users

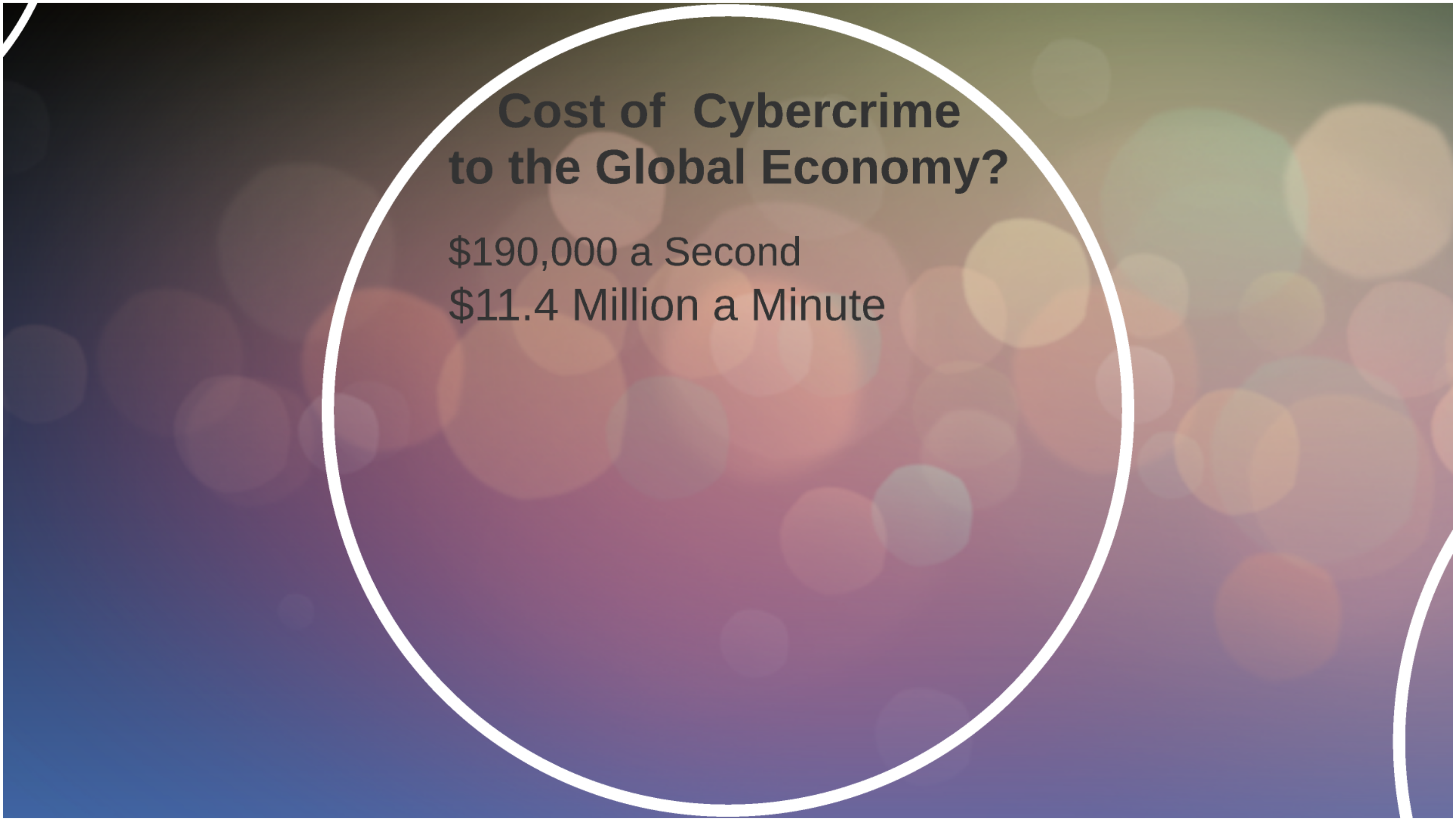
North Korea and China pose a greater Cyber Attack threat than Russia

European Medical Agency saw repeated attacks on COVID 19 vaccine producers

Cost of Cybercrime to the Global Economy?

Cost of Cybercrime to the Global Economy?

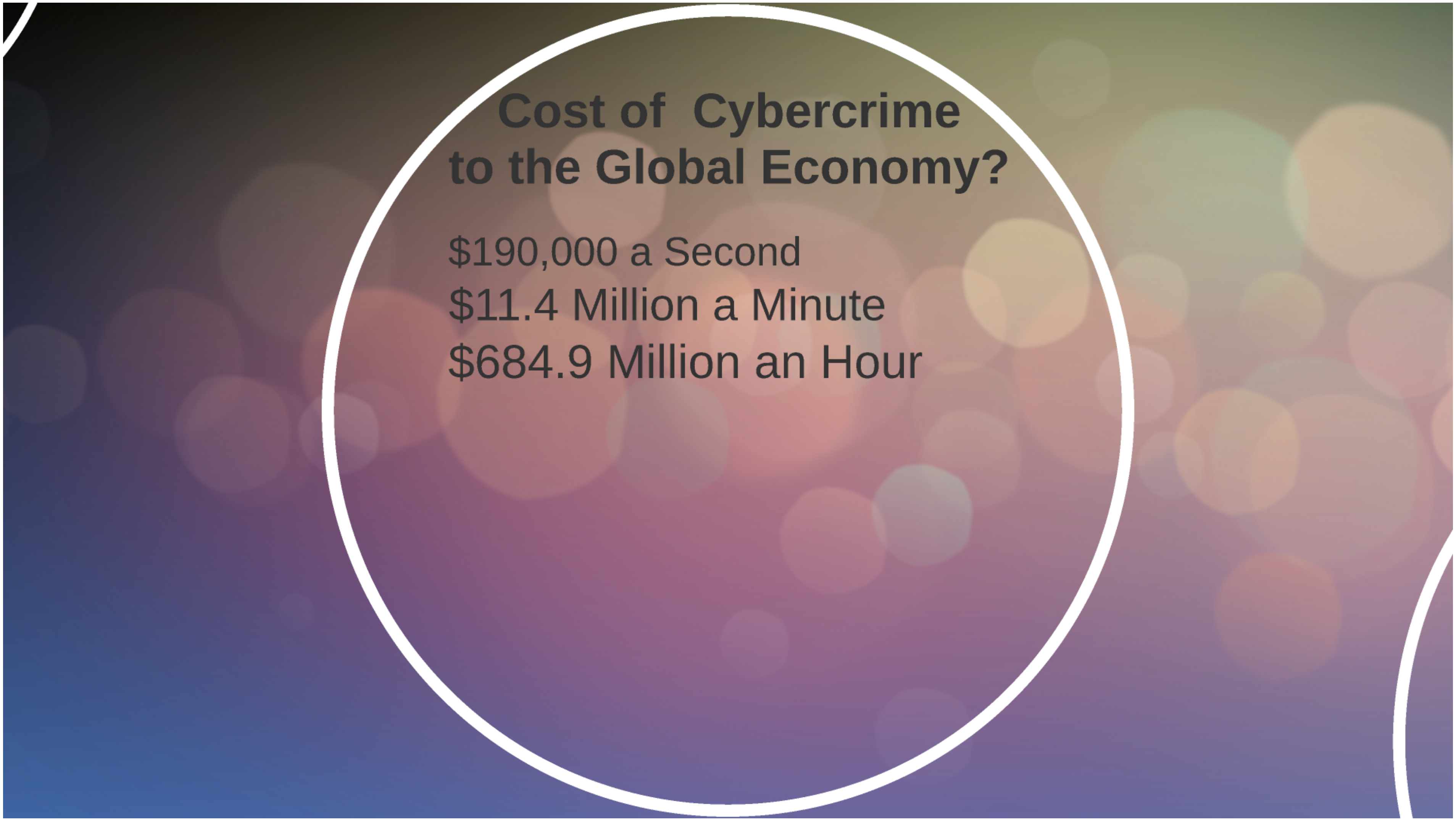
$190,000 a Second



Cost of Cybercrime to the Global Economy?

$190,000 a Second

$11.4 Million a Minute

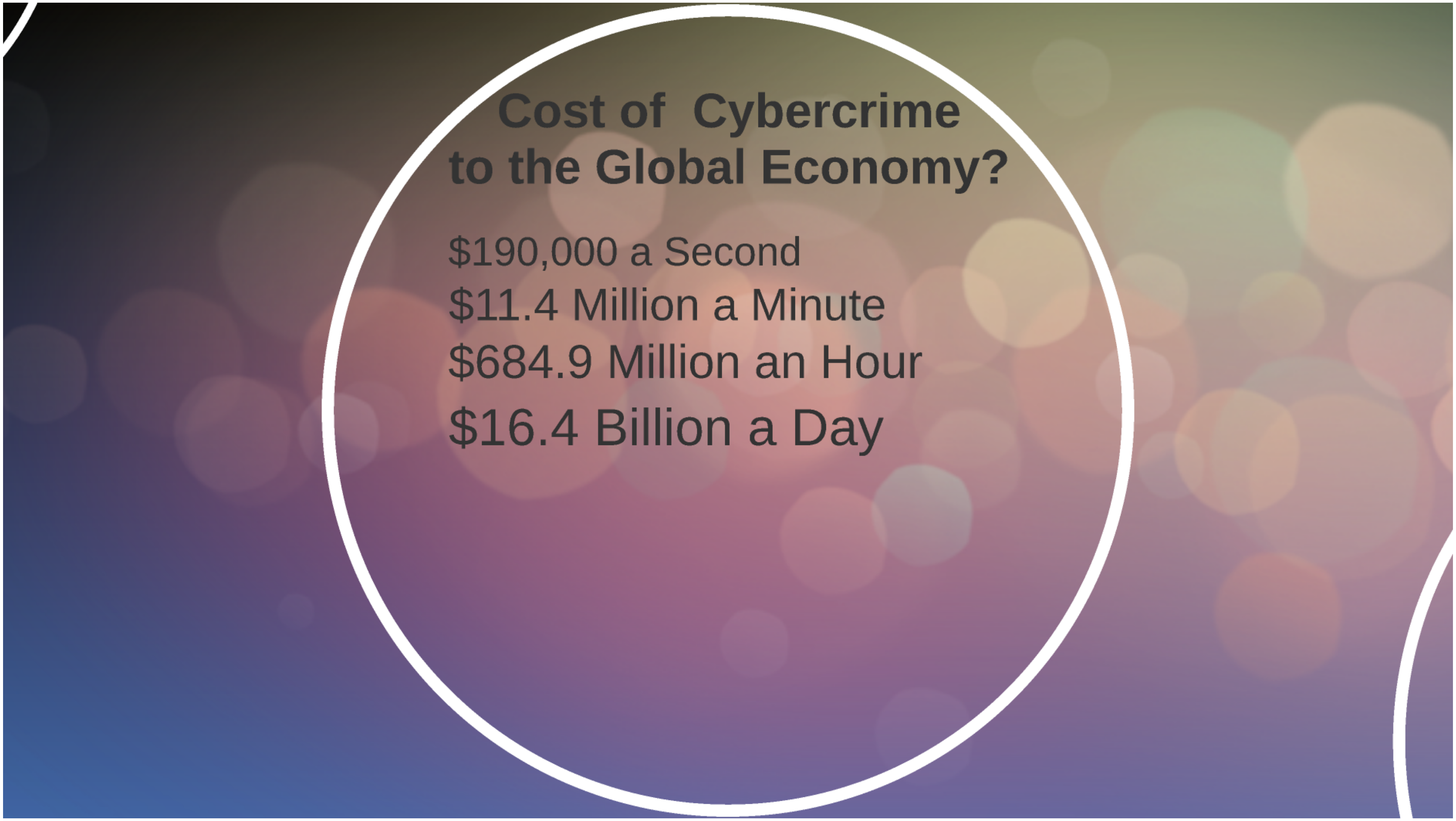


Cost of Cybercrime to the Global Economy?

$190,000 a Second

$11.4 Million a Minute

$684.9 Million an Hour



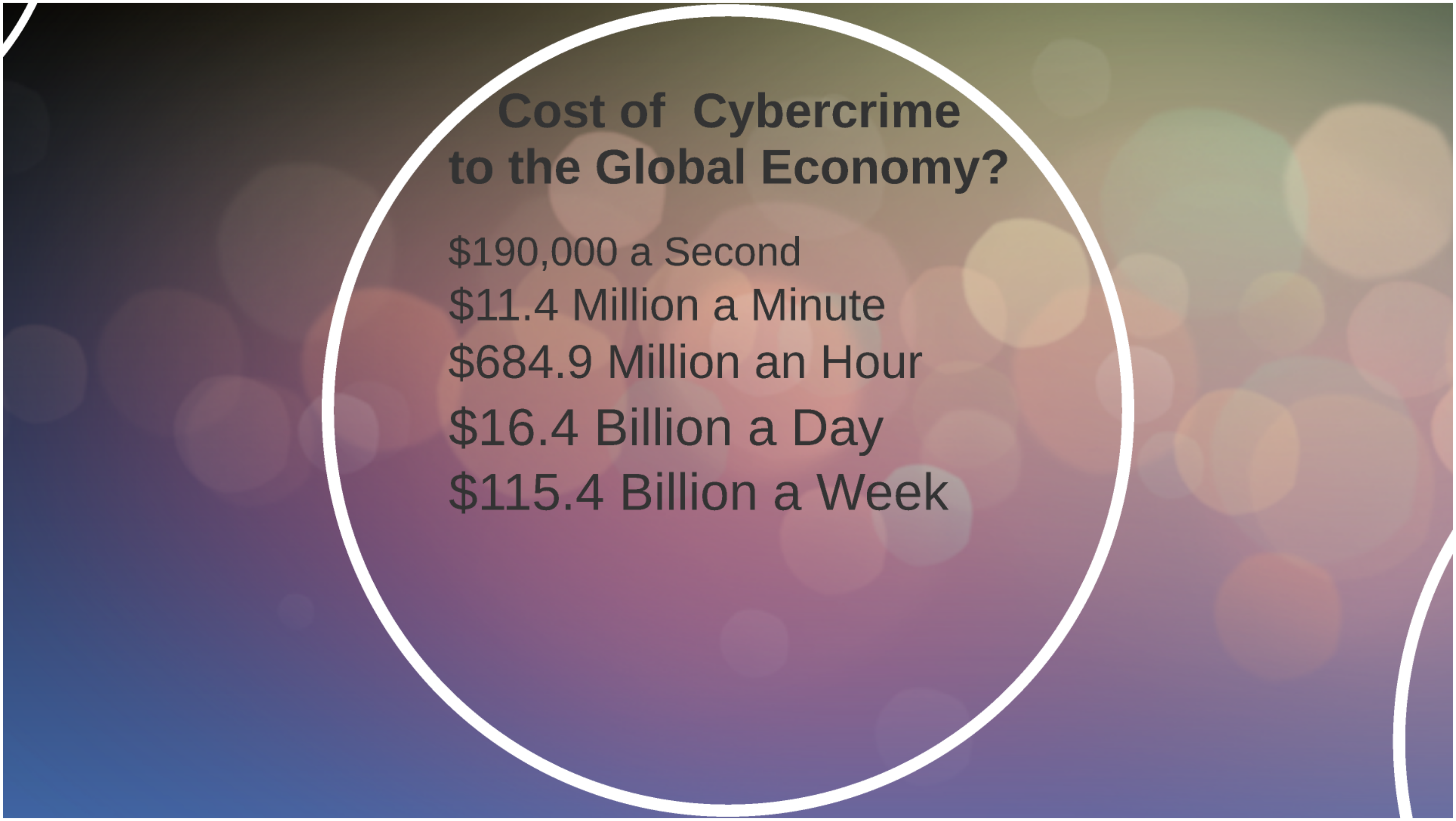
Cost of Cybercrime to the Global Economy?

$190,000 a Second

$11.4 Million a Minute

$684.9 Million an Hour

$16.4 Billion a Day



Cost of Cybercrime to the Global Economy?

$190,000 a Second

$11.4 Million a Minute

$684.9 Million an Hour

$16.4 Billion a Day

$115.4 Billion a Week

Cost of Cybercrime to the Global Economy?

$190,000 a Second

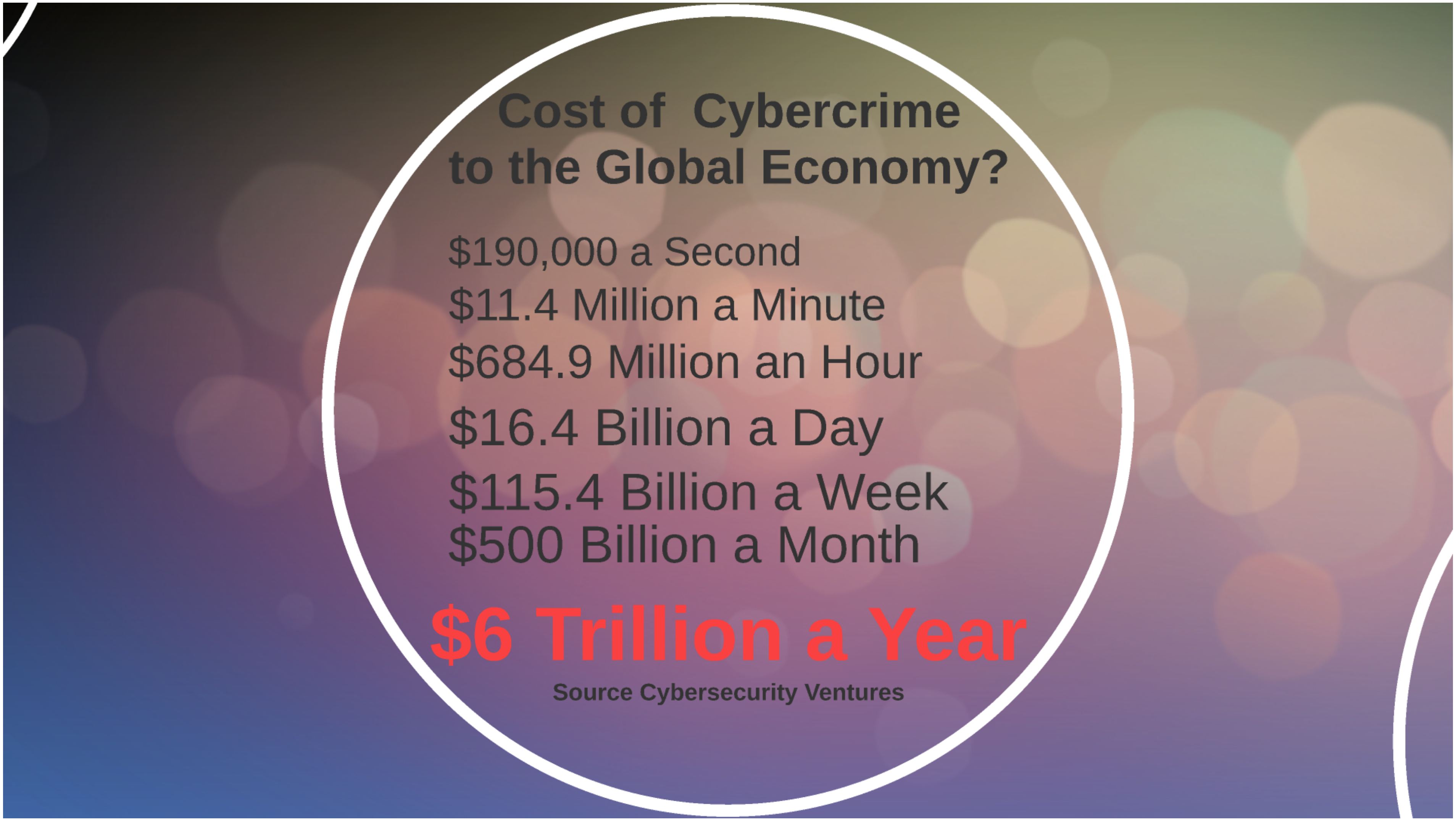
$11.4 Million a Minute

$684.9 Million an Hour

$16.4 Billion a Day

$115.4 Billion a Week

$500 Billion a Month



Cost of Cybercrime to the Global Economy?

$190,000 a Second

$11.4 Million a Minute

$684.9 Million an Hour

$16.4 Billion a Day

$115.4 Billion a Week

$500 Billion a Month

$6 Trillion a Year

Source Cybersecurity Ventures

What is an Ethical Hacker?

What is an Ethical Hacker?

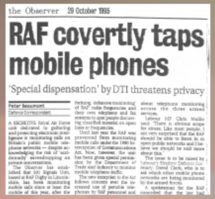
An ethical hacker is a **computer and network expert**, employed to attack a system on behalf of its owners, seeking vulnerabilities a malicious hacker could exploit.

What is the difference between:

an amateur hacker
&
a professional hacker?

network
on behalf
ies a
t.

Our Expertise



the Observer 29 October 1995

RAF covertly taps mobile phones

'Special dispensation' by DTI threatens privacy

Peter Beaumont
Defence Correspondent

A SECRETIVE Royal Air Force unit dedicated to gathering and protecting electronic intelligence is monitoring calls on Britain's public mobile telephone networks — despite acknowledging the risk of 'accidentally' eavesdropping on private conversations.

The Observer has established that 591 Signals Unit, based at RAF Digby in Lincolnshire, has been monitoring mobile calls since at least the middle of this year, after the forming 'defensive monitoring' of RAF radio frequencies and their own telephone and fax systems to spot people discussing classified material on open lines or frequencies.

Until last year the RAF was prevented from monitoring mobile calls under the 1985 Interception of Communications Act. Now, however, the unit has been given special permission by the Department of Trade and Industry to monitor mobile telephone traffic.

The new exemption to the Act follows concern over the increased use of portable telephones by RAF personnel and about telephone monitoring across the three armed services.

Labour MP Chris Mullin said: 'There is obvious scope for abuse. Like most people, I am very surprised that the RAF should be able to listen in to open public networks and I believe we should be told more about this.'

The issue is to be raised by Labour's Shadow Defence Secretary, David Clark, who is to ask which other mobile phone networks are being monitored by the armed forces.

A spokesman for the RAF conceded that the law had

Source: Observer 29th October 1995

Good Practice Guide for Computer-Based Electronic Evidence

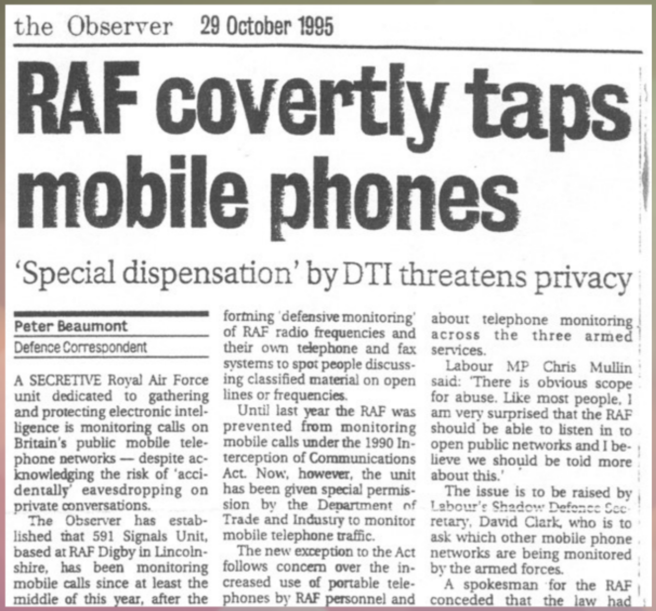
Official release version 4.0

http://www.7safe.com/electronic_evidence/
ACPO_guidelines_computer_evidence_v4_web.pdf

Certifications

Certified Forensic Investigation Practitioner · Computer Forensics
CFIP

Certified Security Testing Associate · Ethical Hacking
CSTA



the Observer 29 October 1995

RAF covertly taps mobile phones

'Special dispensation' by DTI threatens privacy

Peter Beaumont
Defence Correspondent

A SECRETIVE Royal Air Force unit dedicated to gathering and protecting electronic intelligence is monitoring calls on Britain's public mobile telephone networks — despite acknowledging the risk of 'accidentally' eavesdropping on private conversations.

The Observer has established that 591 Signals Unit, based at RAF Digby in Lincolnshire, has been monitoring mobile calls since at least the middle of this year, after the forming 'defensive monitoring' of RAF radio frequencies and their own telephone and fax systems to spot people discussing classified material on open lines or frequencies.

Until last year the RAF was prevented from monitoring mobile calls under the 1990 Interception of Communications Act. Now, however, the unit has been given special permission by the Department of Trade and Industry to monitor mobile telephone traffic.

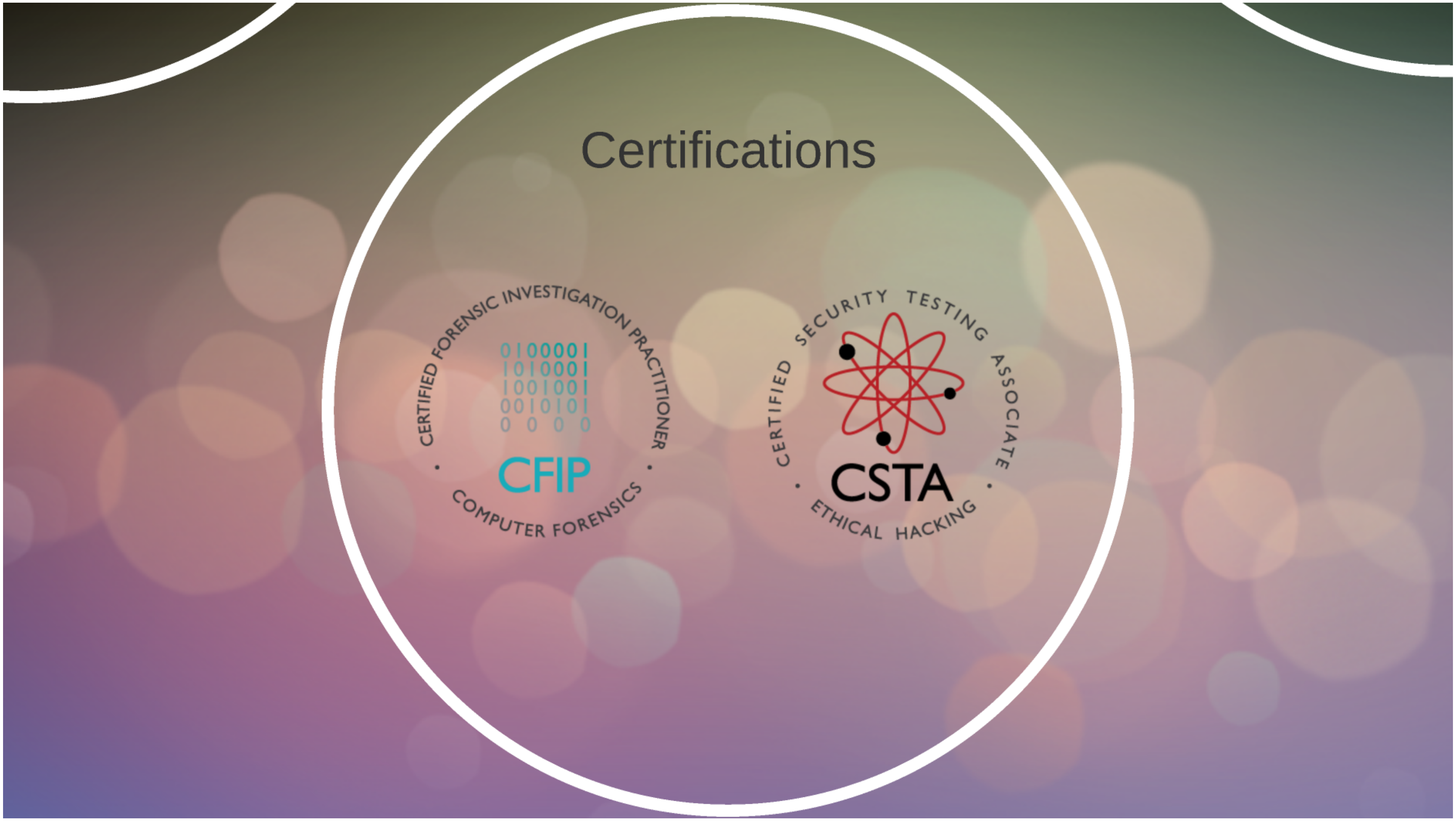
The new exception to the Act follows concern over the increased use of portable telephones by RAF personnel and about telephone monitoring across the three armed services.

Labour MP Chris Mullin said: 'There is obvious scope for abuse. Like most people, I am very surprised that the RAF should be able to listen in to open public networks and I believe we should be told more about this.'

The issue is to be raised by Labour's Shadow Defence Secretary, David Clark, who is to ask which other mobile phone networks are being monitored by the armed forces.

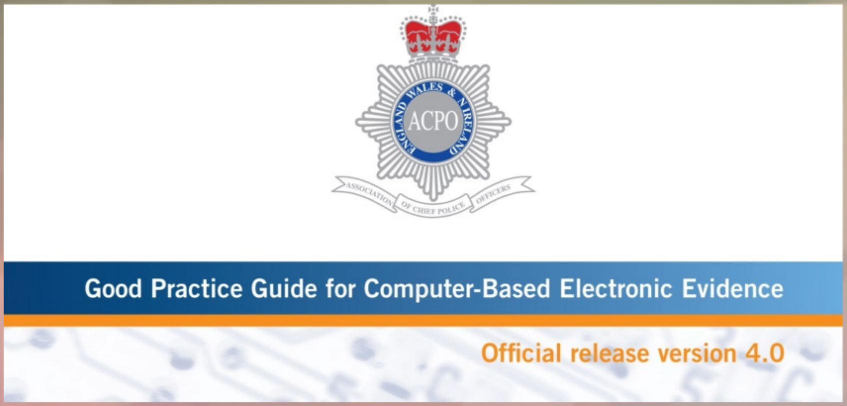
A spokesman for the RAF conceded that the law had

Source: Observer 29th October 1995



Certifications

CERTIFIED FORENSIC INVESTIGATION PRACTITIONER
0100001
1010001
1001001
0010101
0 0 0 0
CFIP
COMPUTER FORENSICS
CERTIFIED SECURITY TESTING ASSOCIATE
CSTA
ETHICAL HACKING



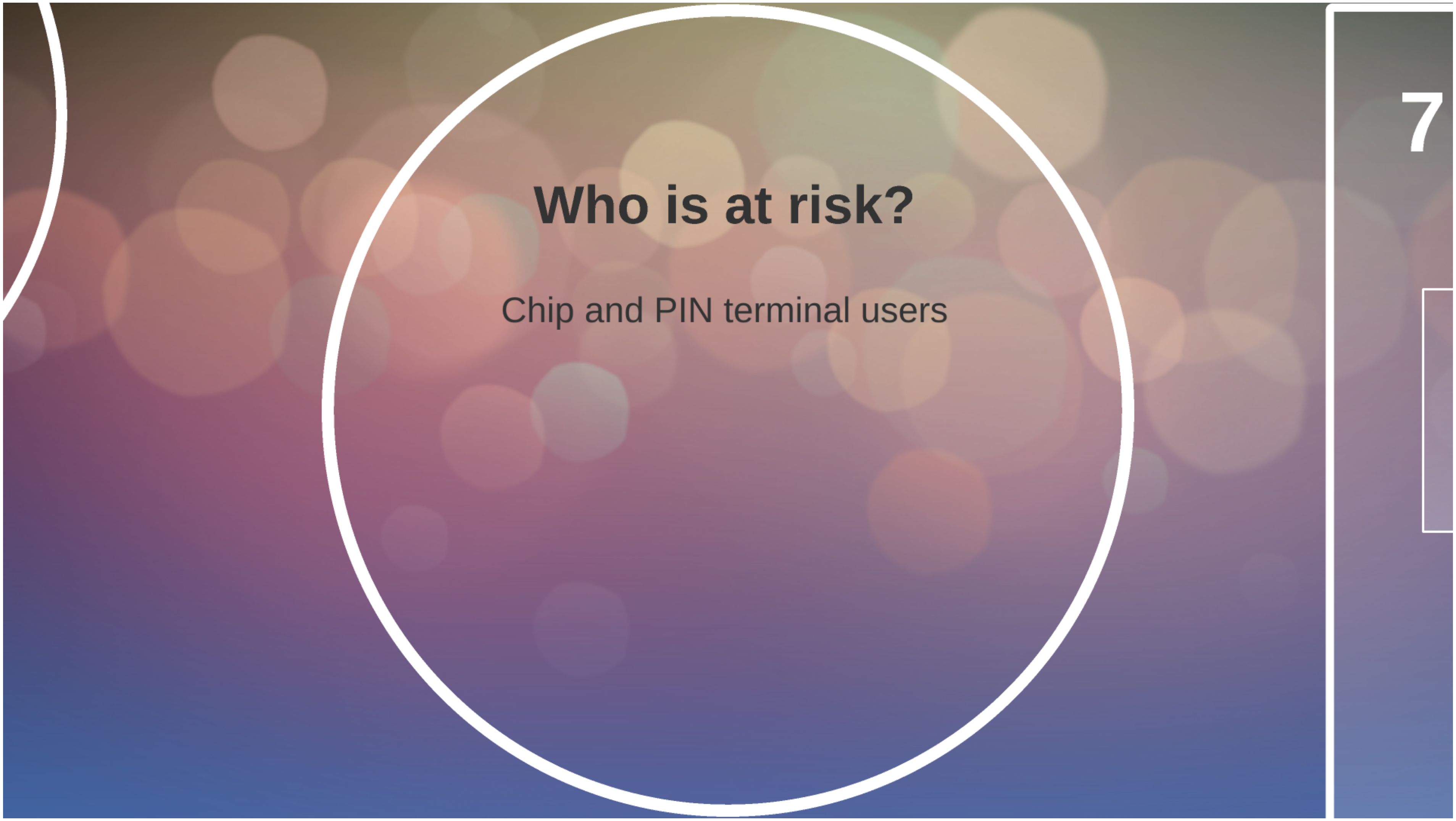
Good Practice Guide for Computer-Based Electronic Evidence

Official release version 4.0

http://www.7safe.com/electronic_evidence/
ACPO_guidelines_computer_evidence_v4_web.pdf

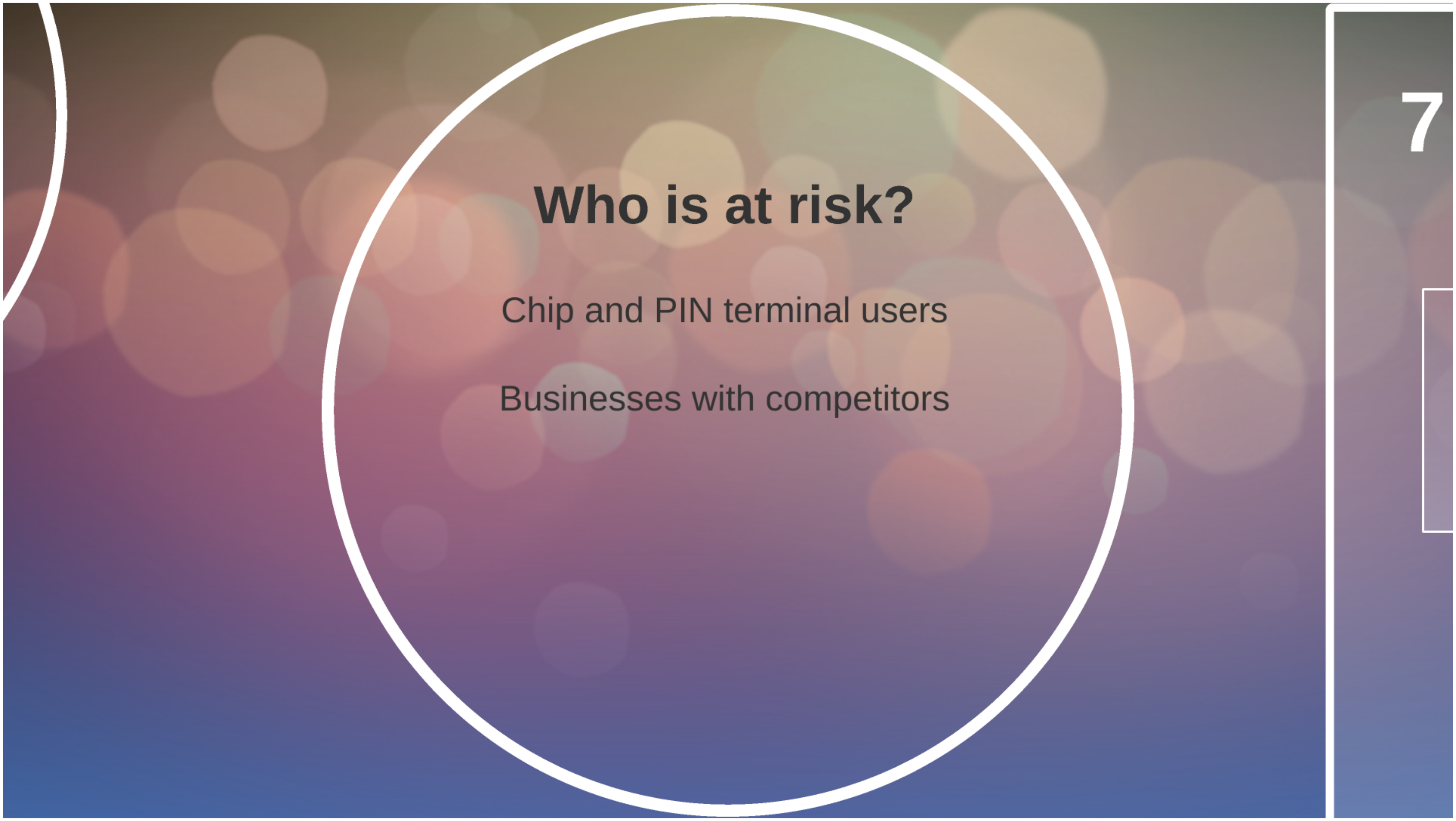
Who is at risk?

7



Who is at risk?

Chip and PIN terminal users



Who is at risk?

Chip and PIN terminal users

Businesses with competitors

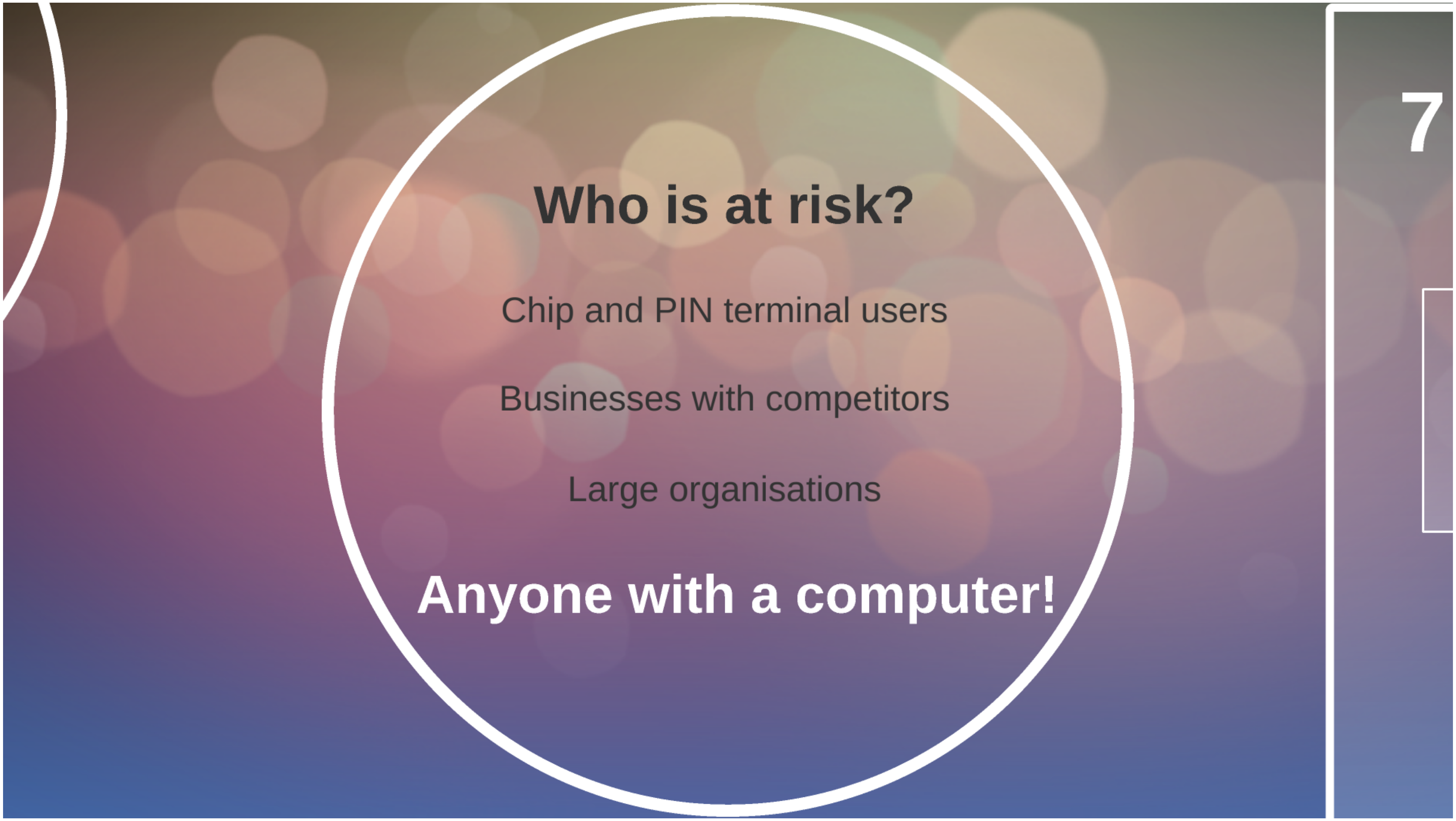
Who is at risk?

Chip and PIN terminal users

Businesses with competitors

Large organisations

7



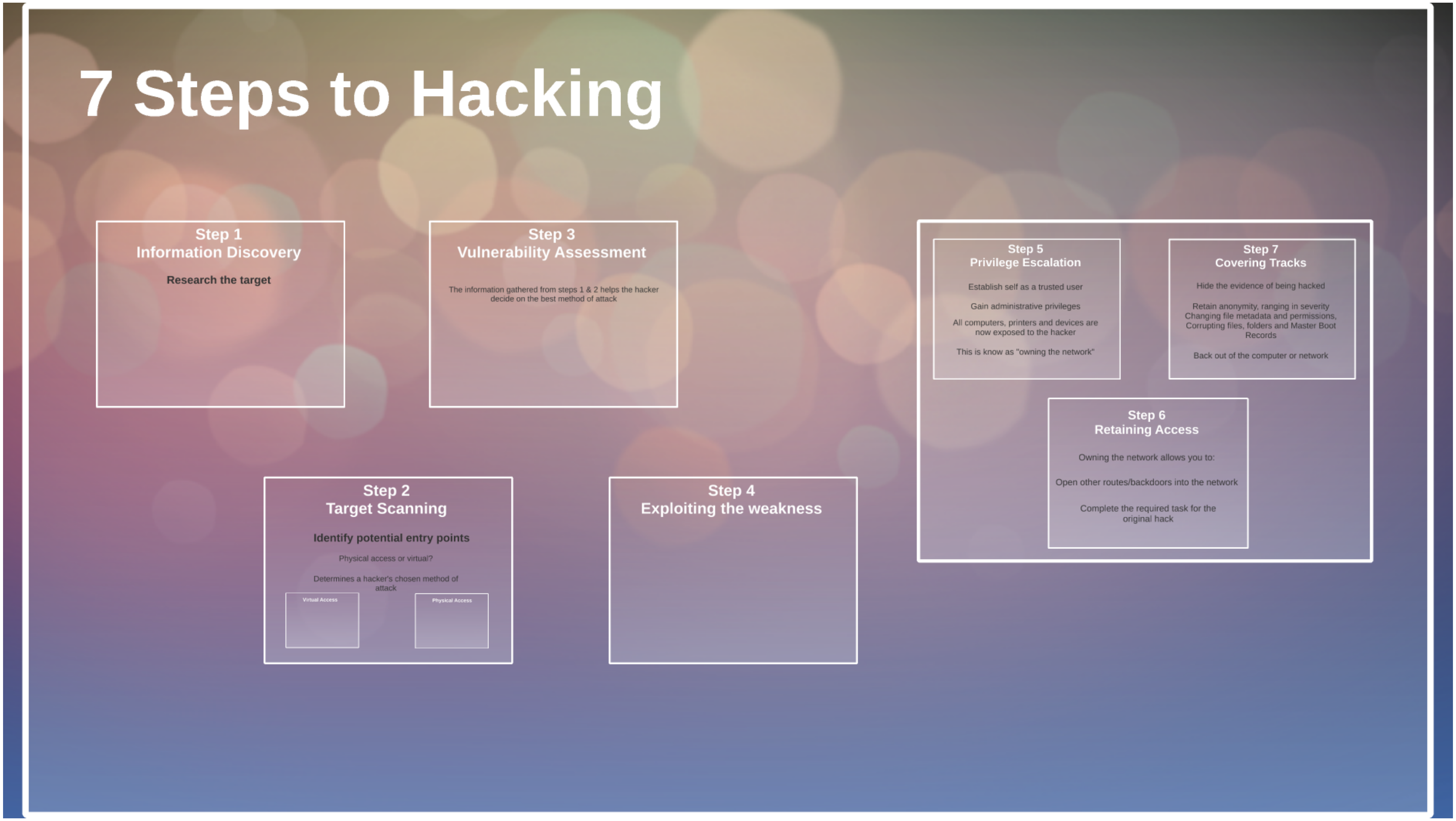
Who is at risk?

Chip and PIN terminal users

Businesses with competitors

Large organisations

Anyone with a computer!



7 Steps to Hacking

Step 1
Information Discovery

Research the target

Step 2
Target Scanning

Identify potential entry points

Physical access or virtual?

Determines a hacker's chosen method of attack

Virtual Access

Physical Access

Step 3
Vulnerability Assessment

The information gathered from steps 1 & 2 helps the hacker decide on the best method of attack

Step 4
Exploiting the weakness

Step 5
Privilege Escalation

Establish self as a trusted user

Gain administrative privileges

All computers, printers and devices are now exposed to the hacker

This is know as "owning the network"

Step 6
Retaining Access

Owning the network allows you to:

Open other routes/backdoors into the network

Complete the required task for the original hack

Step 7
Covering Tracks

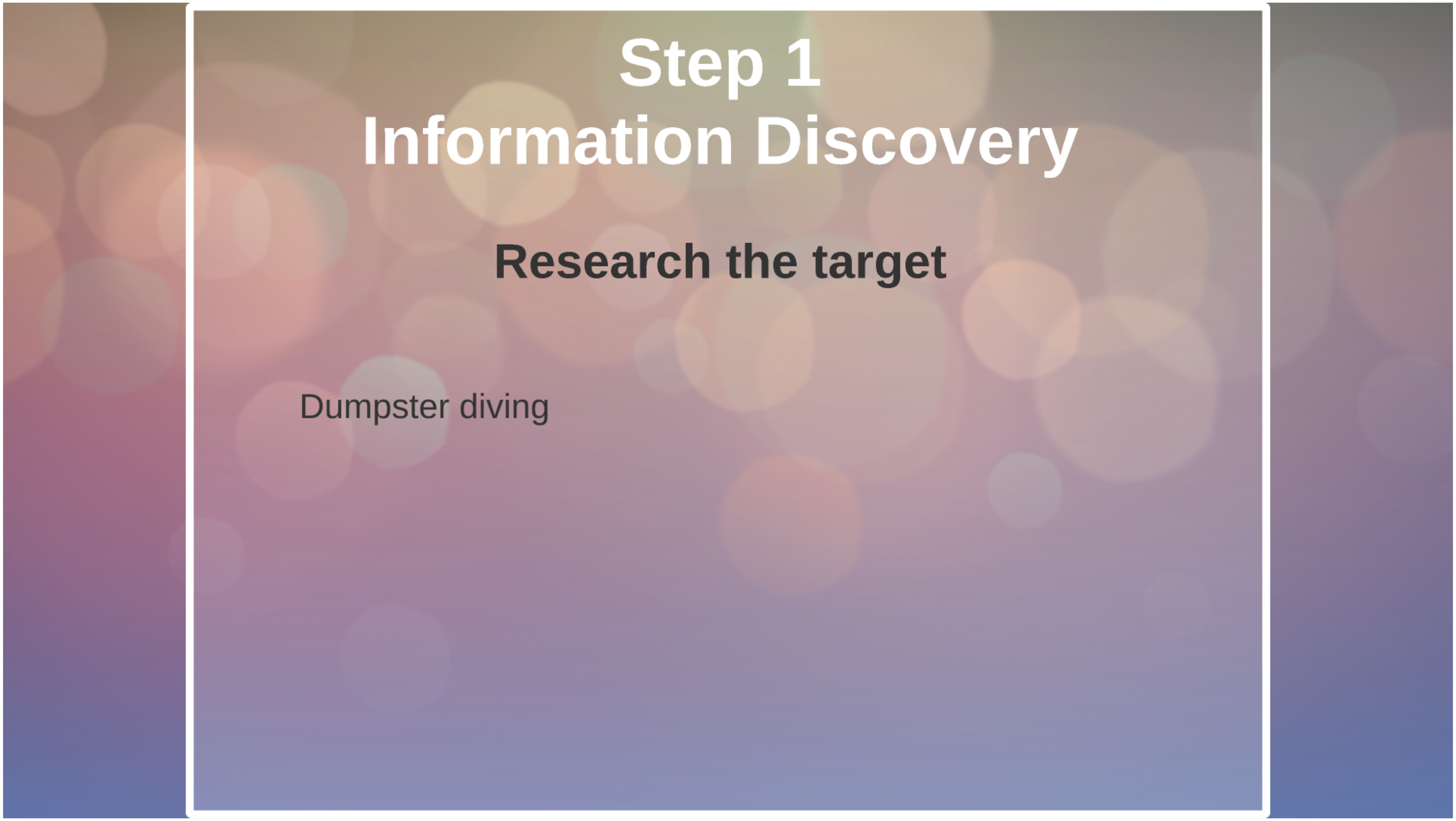
Hide the evidence of being hacked

Retain anonymity, ranging in severity
Changing file metadata and permissions,
Corrupting files, folders and Master Boot Records

Back out of the computer or network

Step 1
Information Discovery

Research the target



Step 1
Information Discovery

Research the target

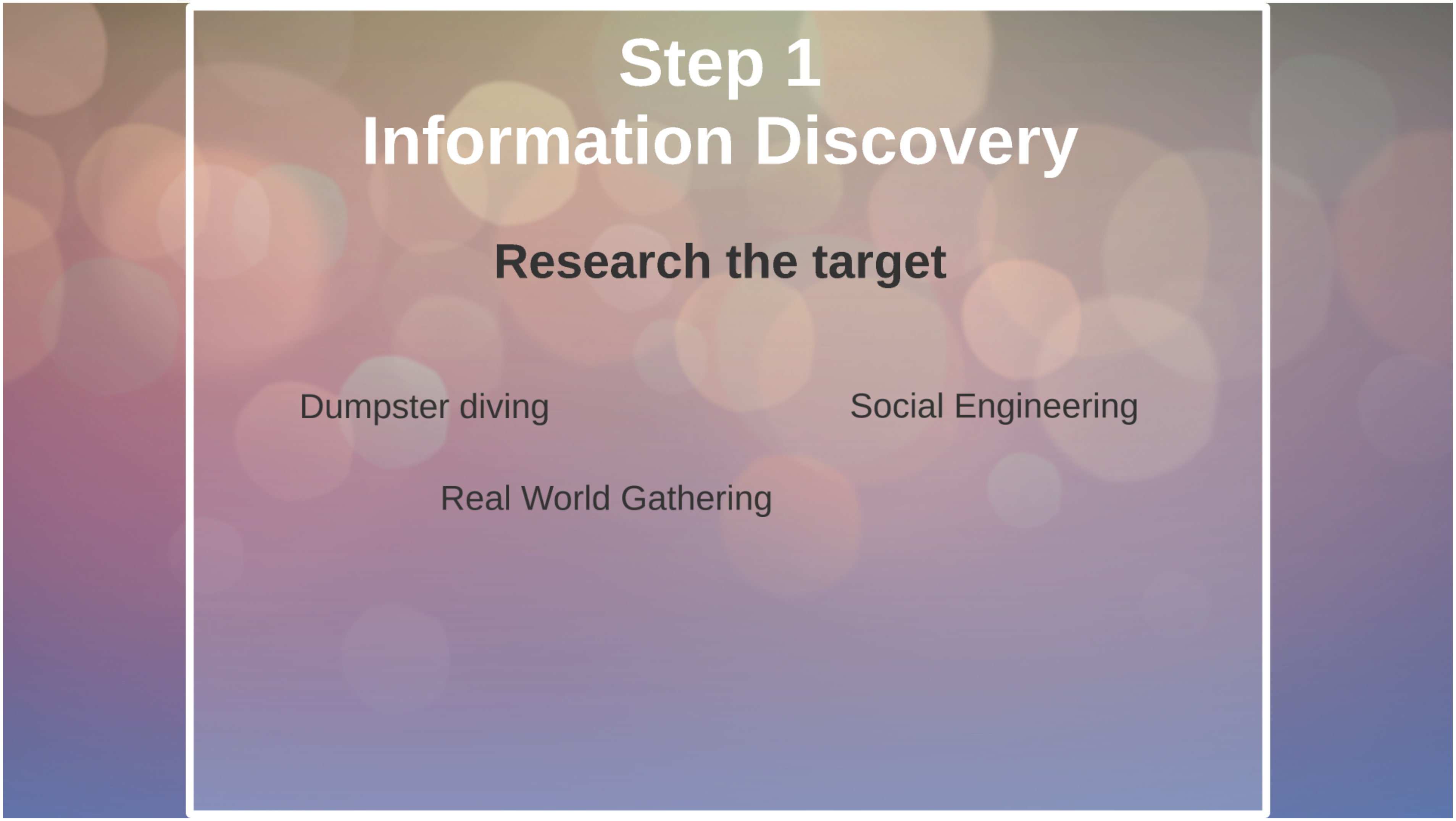
Dumpster diving

Step 1
Information Discovery

Research the target

Dumpster diving

Social Engineering



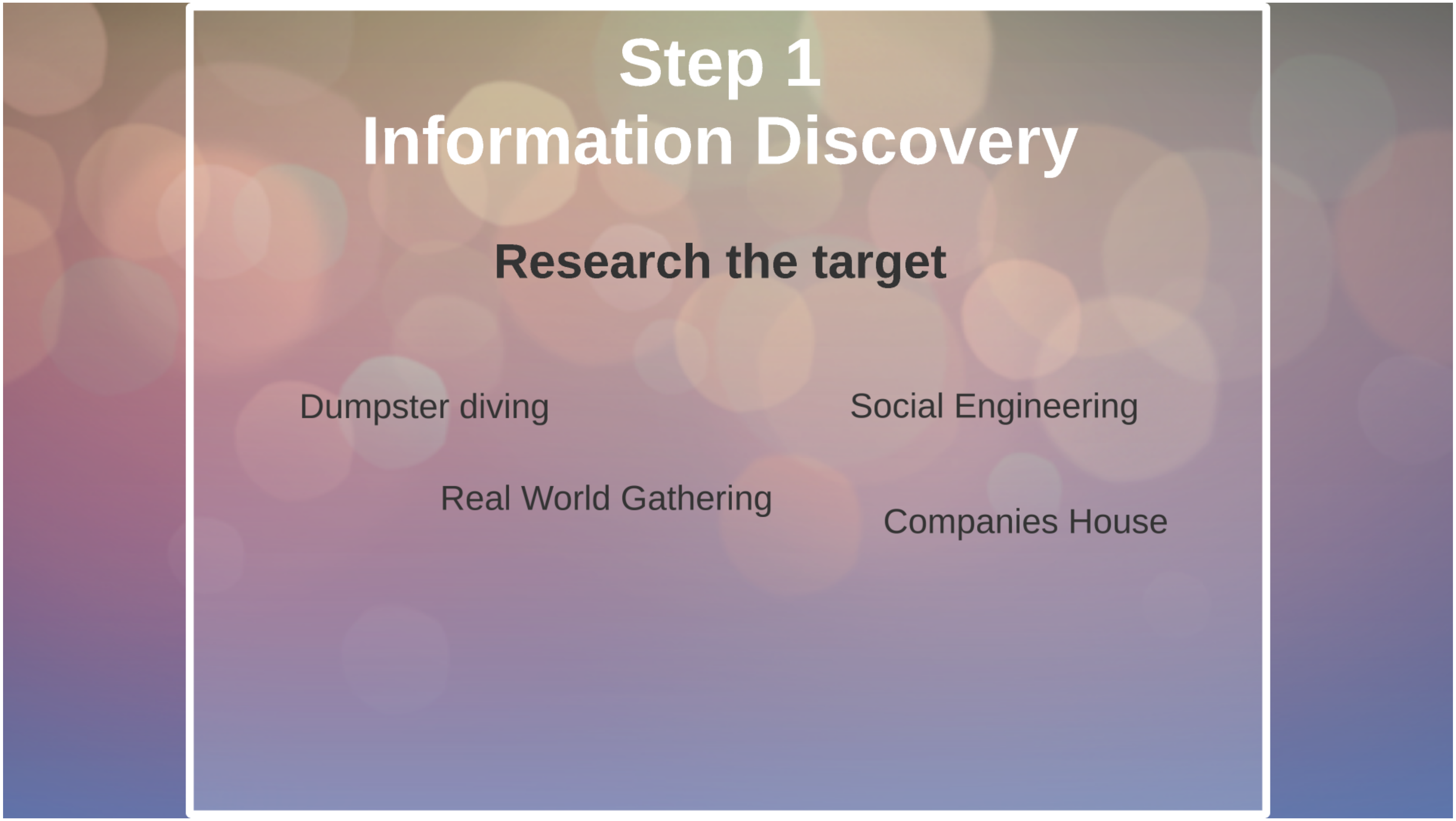
Step 1
Information Discovery

Research the target

Dumpster diving

Social Engineering

Real World Gathering



Step 1
Information Discovery

Research the target

Dumpster diving

Social Engineering

Real World Gathering

Companies House

Step 1
Information Discovery

Research the target

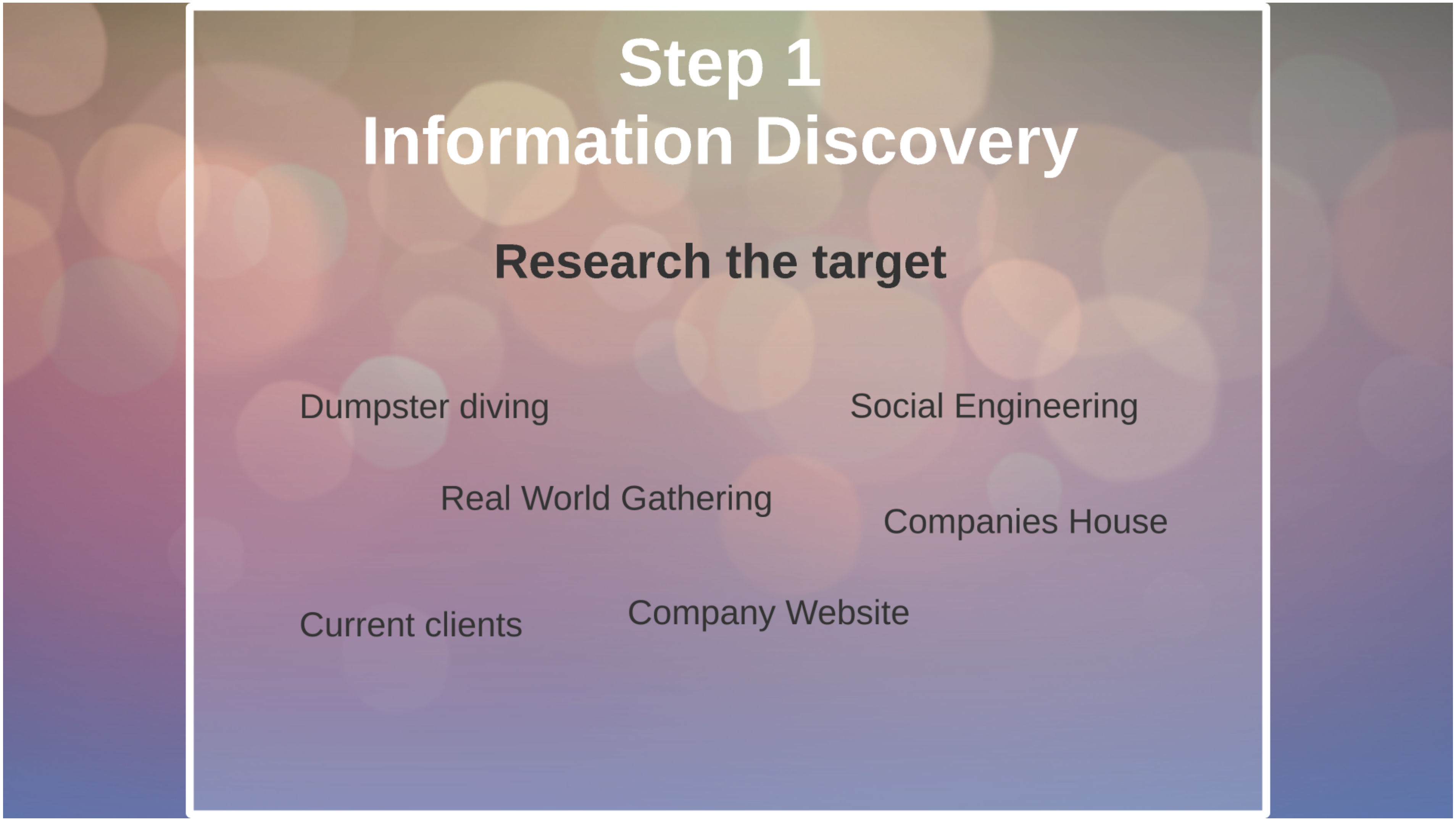
Dumpster diving

Social Engineering

Real World Gathering

Companies House

Current clients



Step 1
Information Discovery

Research the target

Dumpster diving

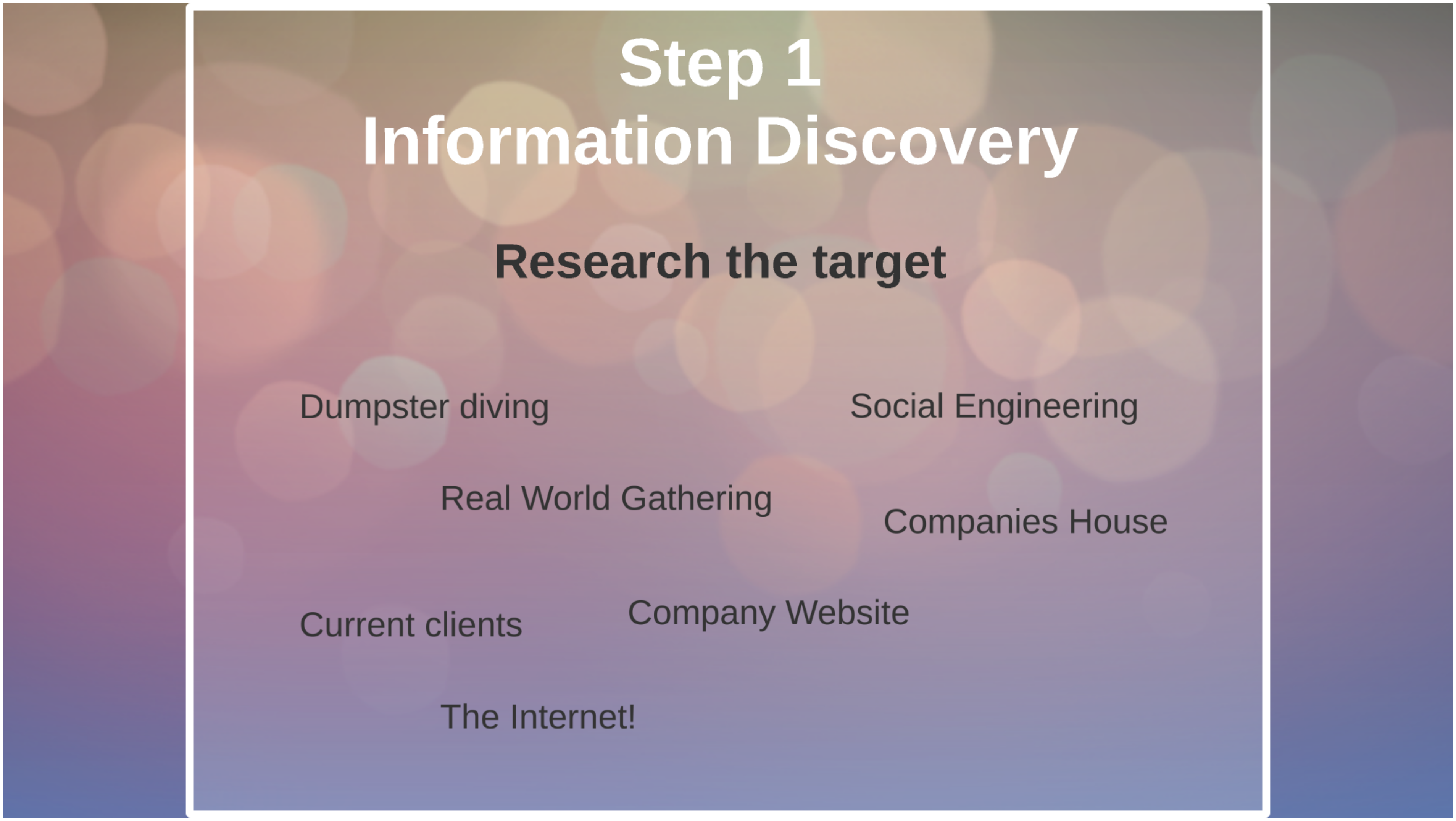
Social Engineering

Real World Gathering

Companies House

Company Website

Current clients



Step 1
Information Discovery

Research the target

Dumpster diving

Social Engineering

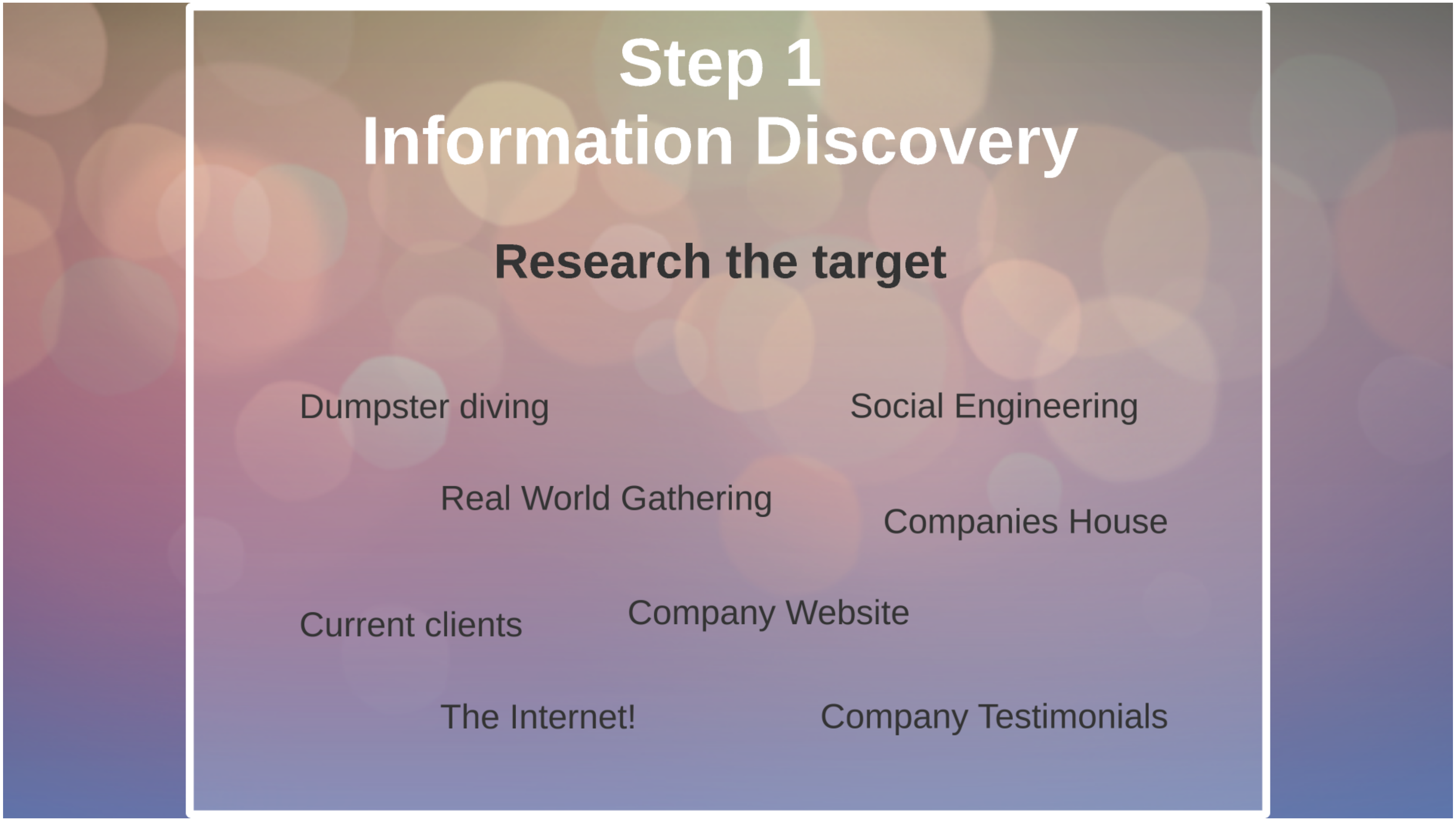
Real World Gathering

Companies House

Current clients

Company Website

The Internet!



Step 1
Information Discovery

Research the target

Dumpster diving

Social Engineering

Real World Gathering

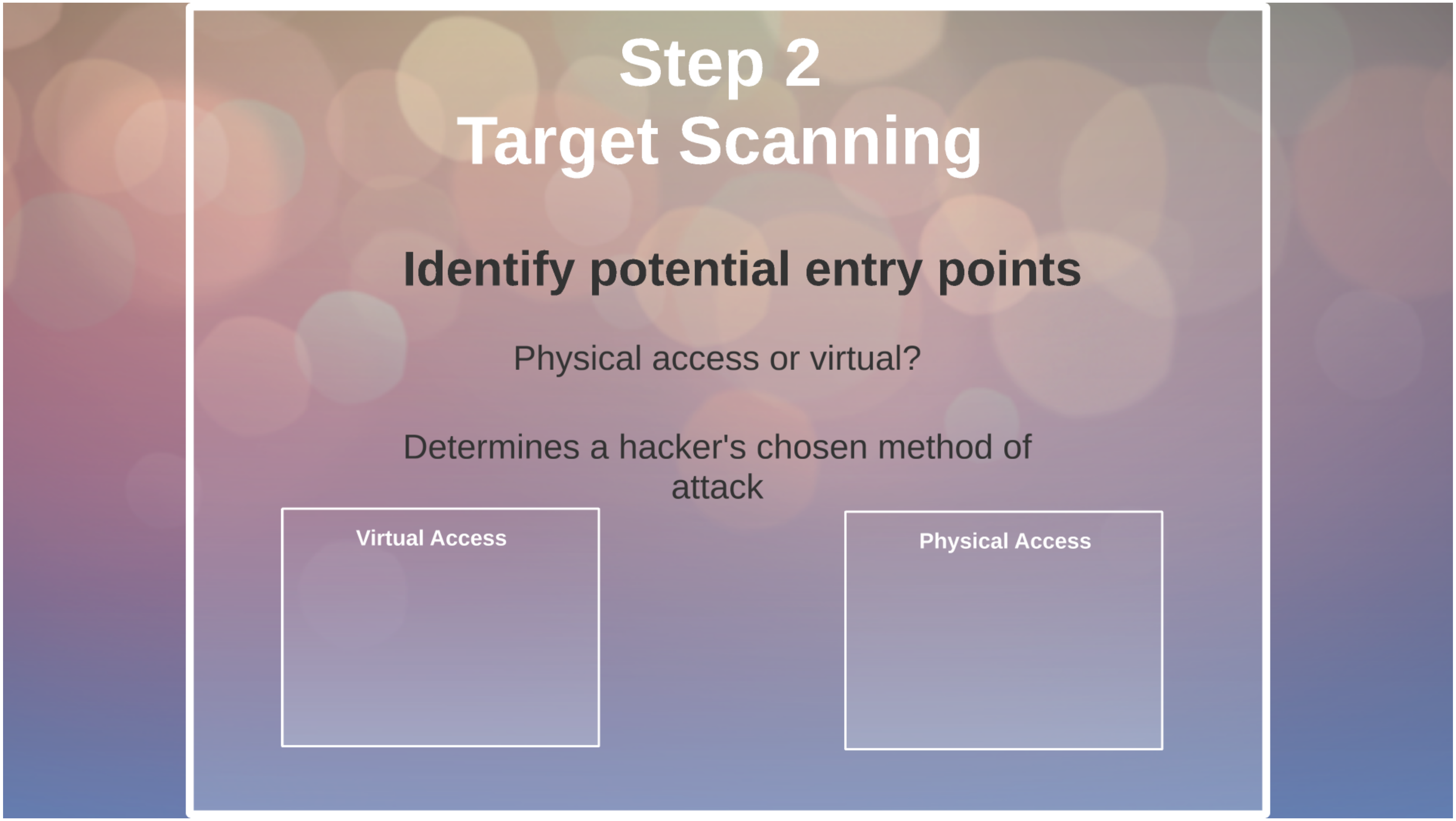
Companies House

Current clients

Company Website

The Internet!

Company Testimonials



Step 2
Target Scanning

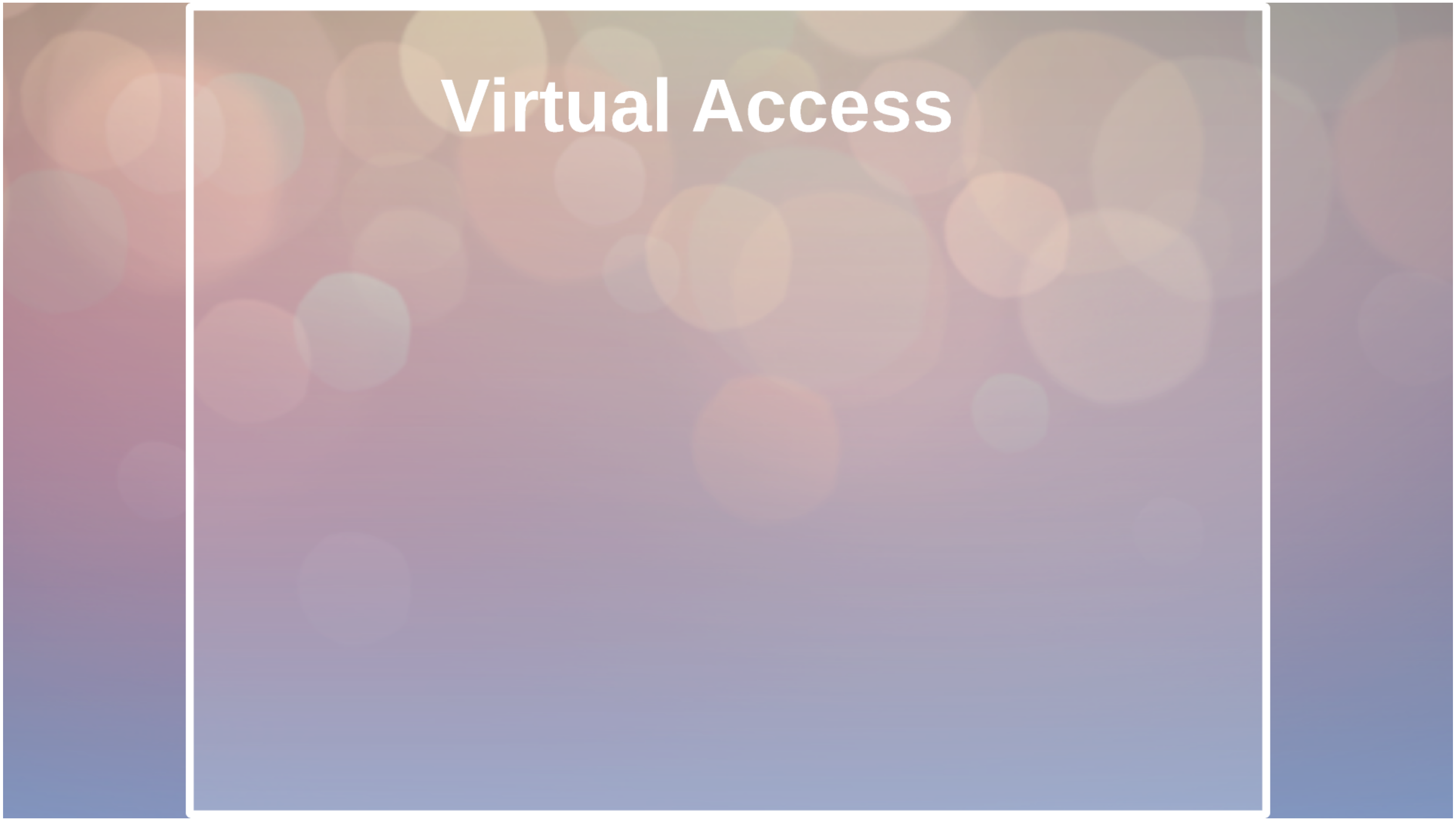
Identify potential entry points

Physical access or virtual?

Determines a hacker's chosen method of attack

Virtual Access

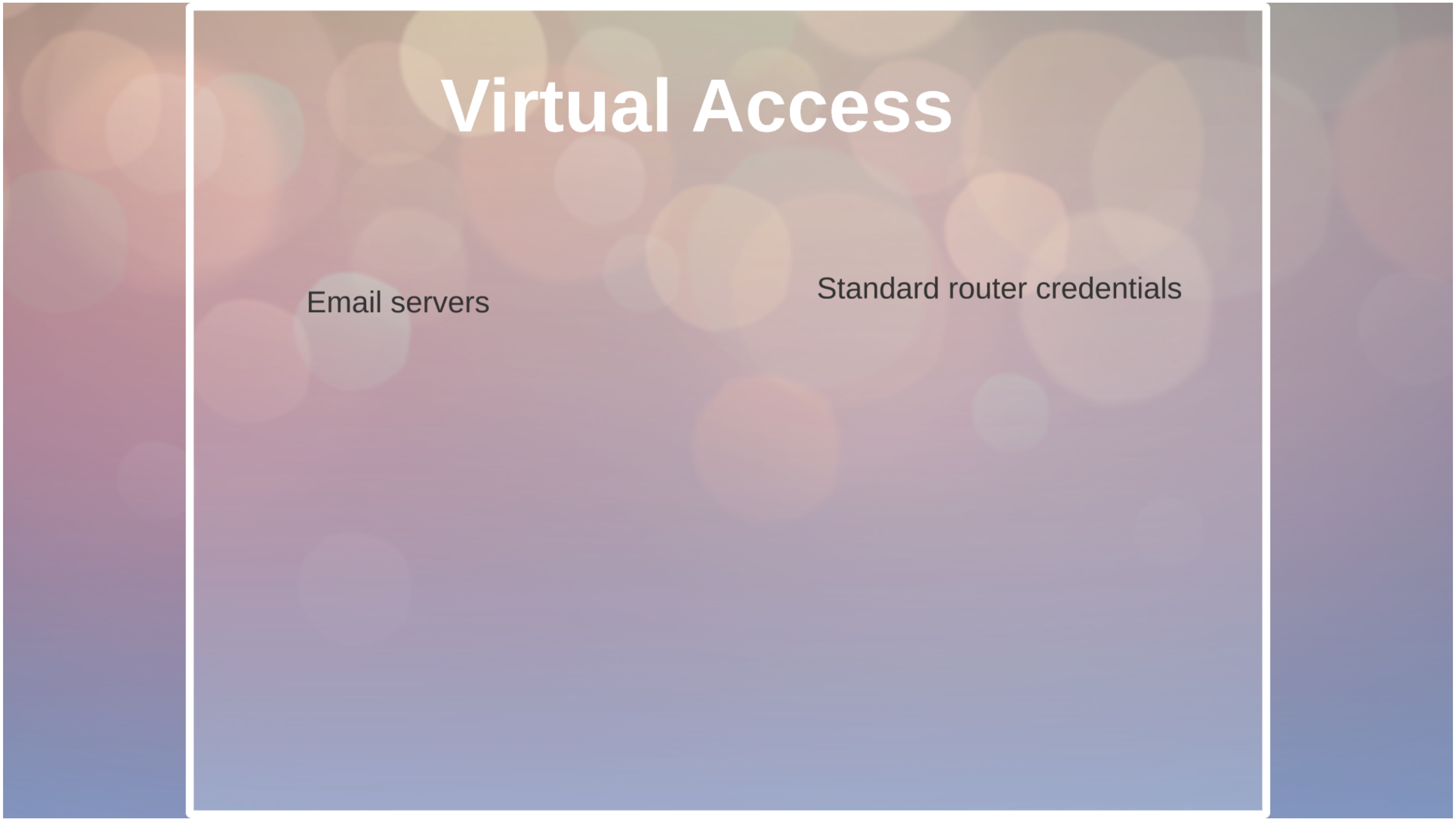
Physical Access



Virtual Access

Virtual Access

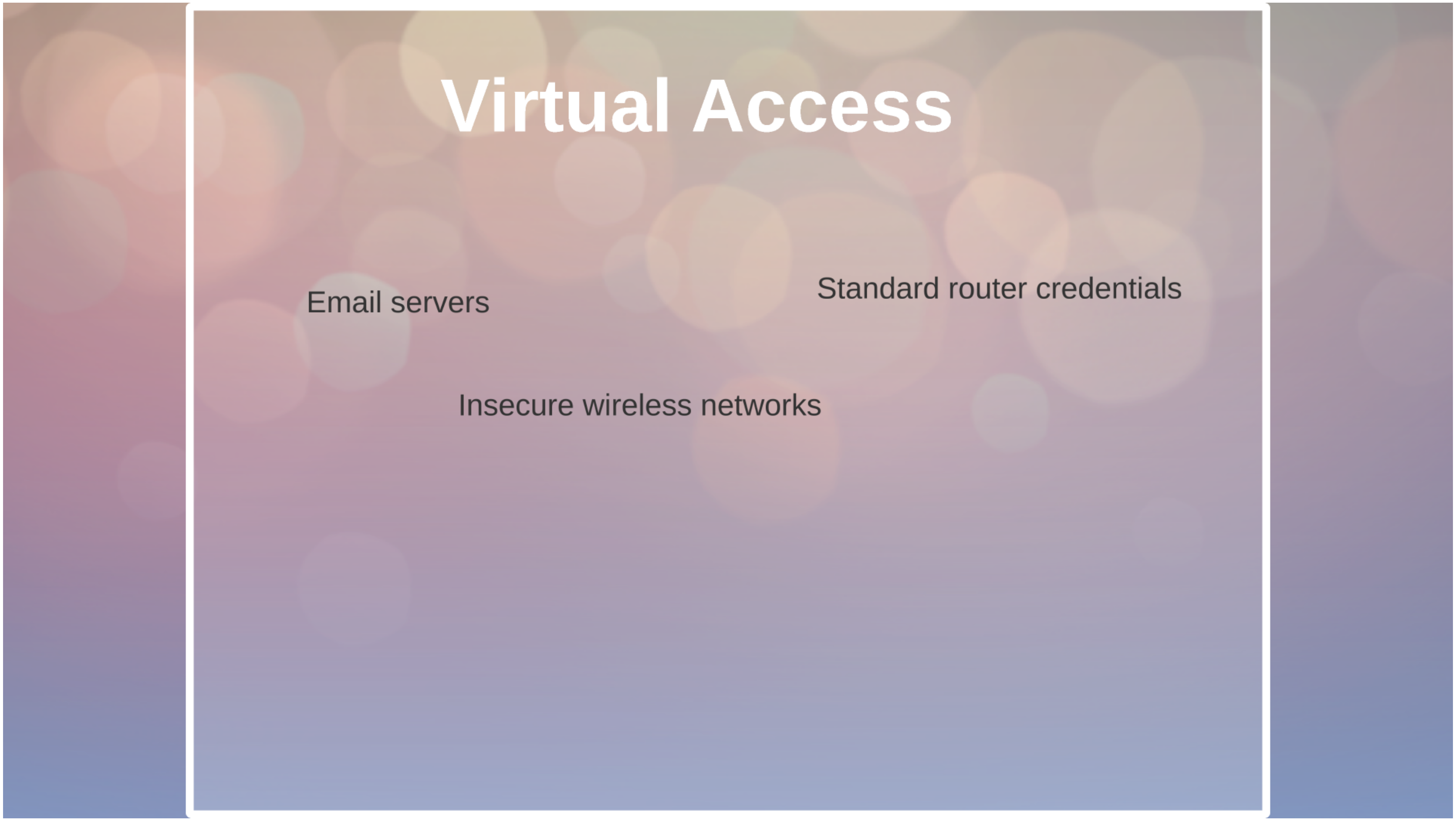
Email servers



Virtual Access

Email servers

Standard router credentials

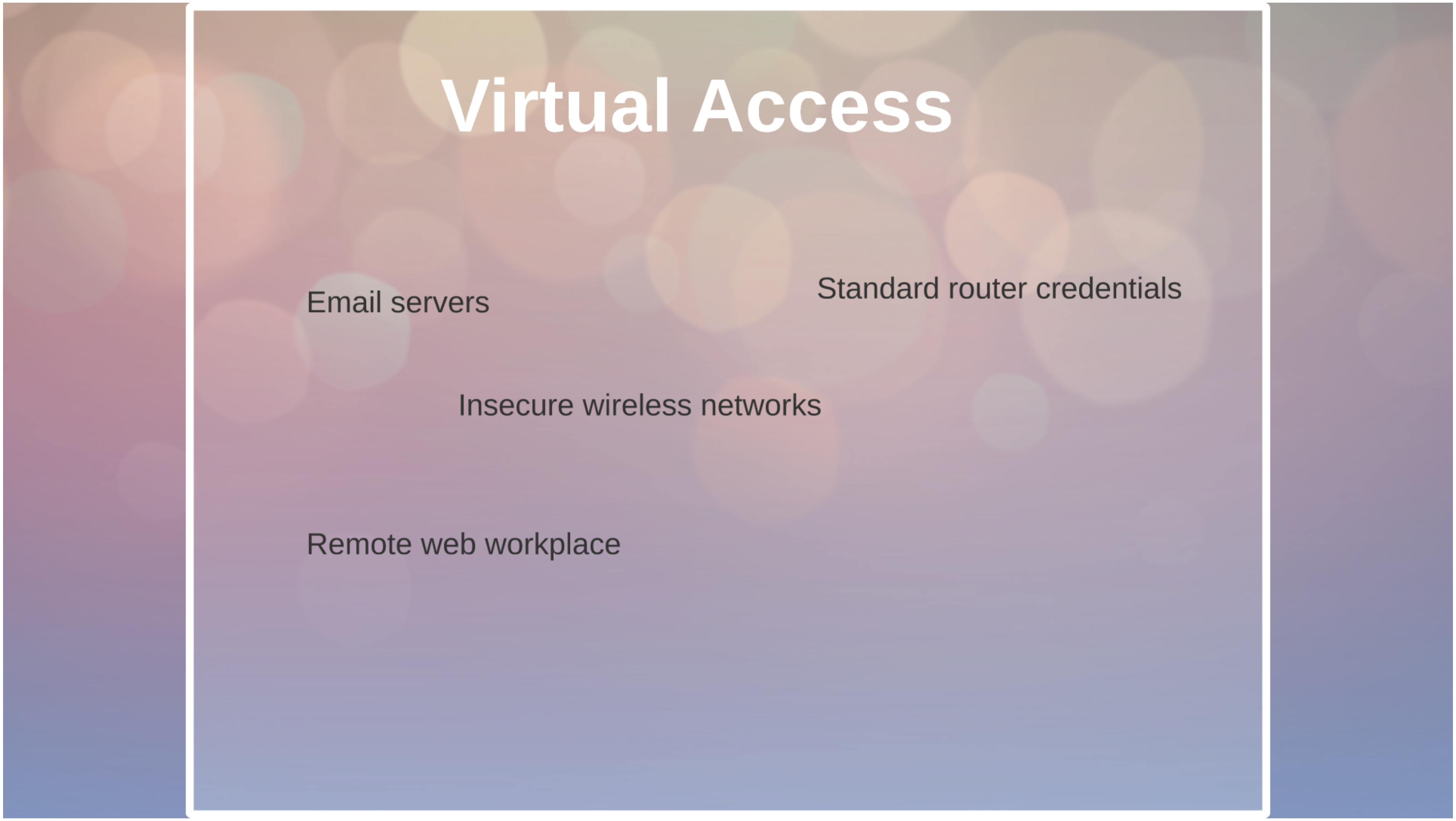


Virtual Access

Email servers

Standard router credentials

Insecure wireless networks



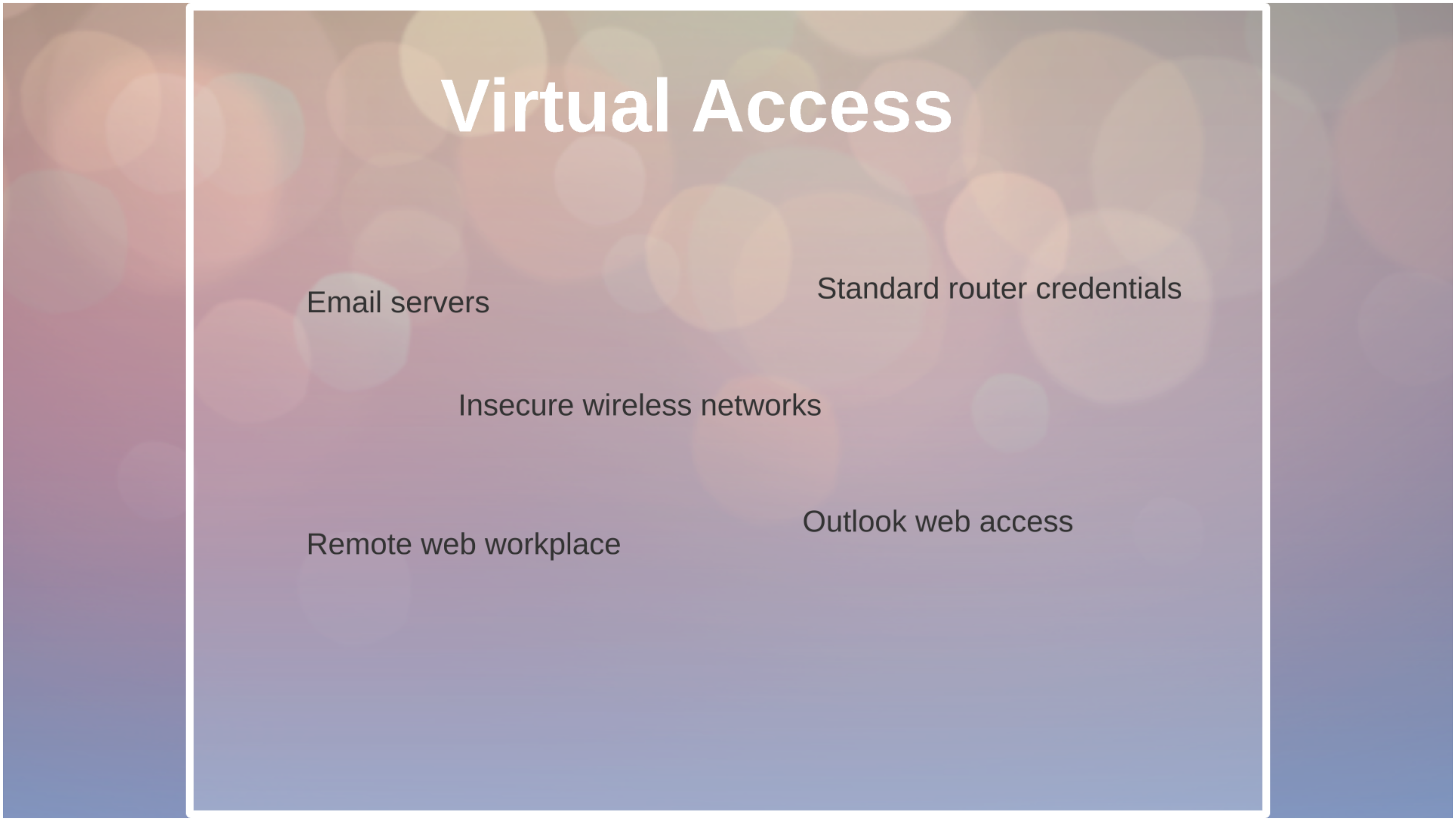
Virtual Access

Email servers

Standard router credentials

Insecure wireless networks

Remote web workplace



Virtual Access

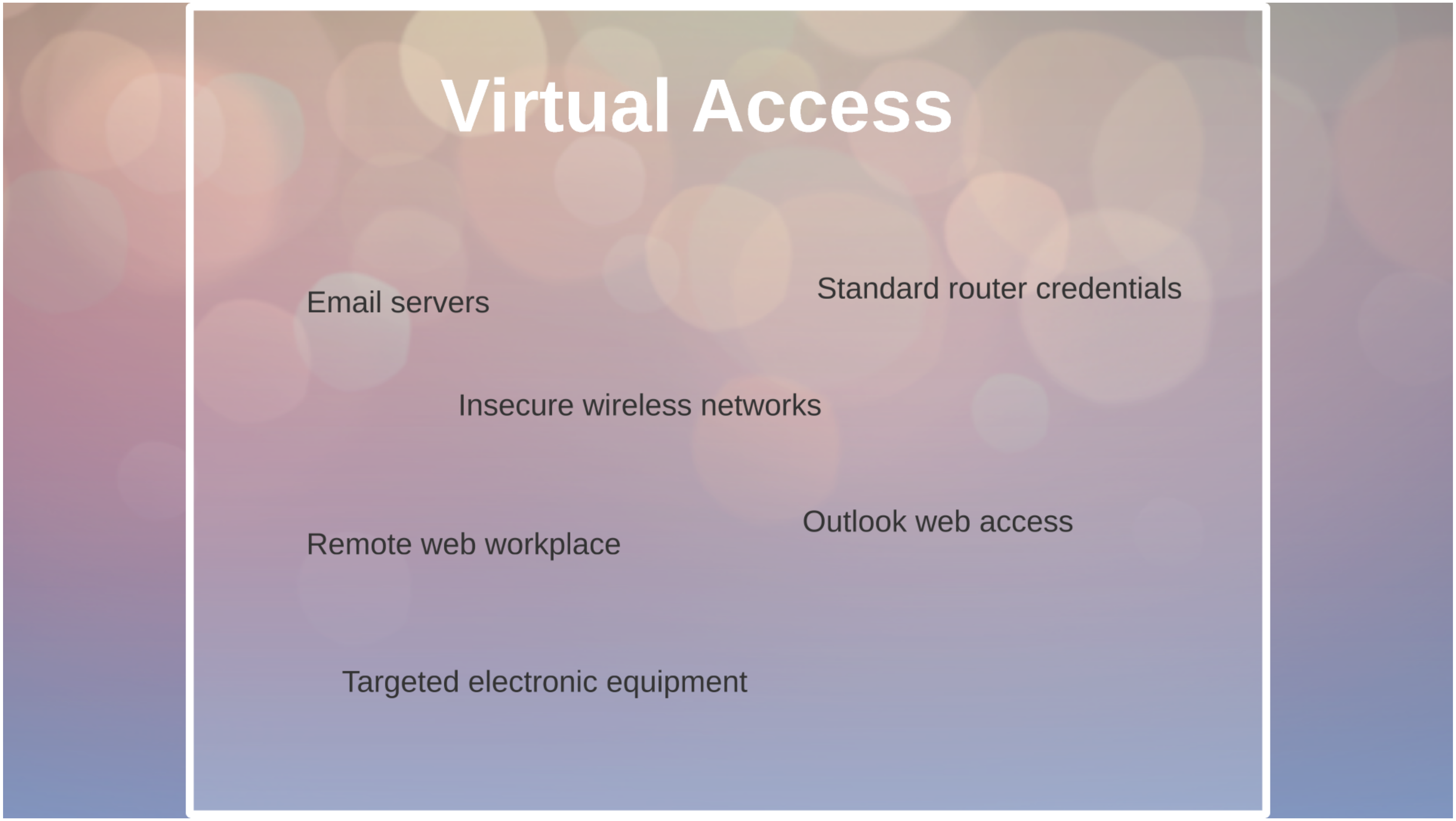
Email servers

Standard router credentials

Insecure wireless networks

Remote web workplace

Outlook web access



Virtual Access

Email servers

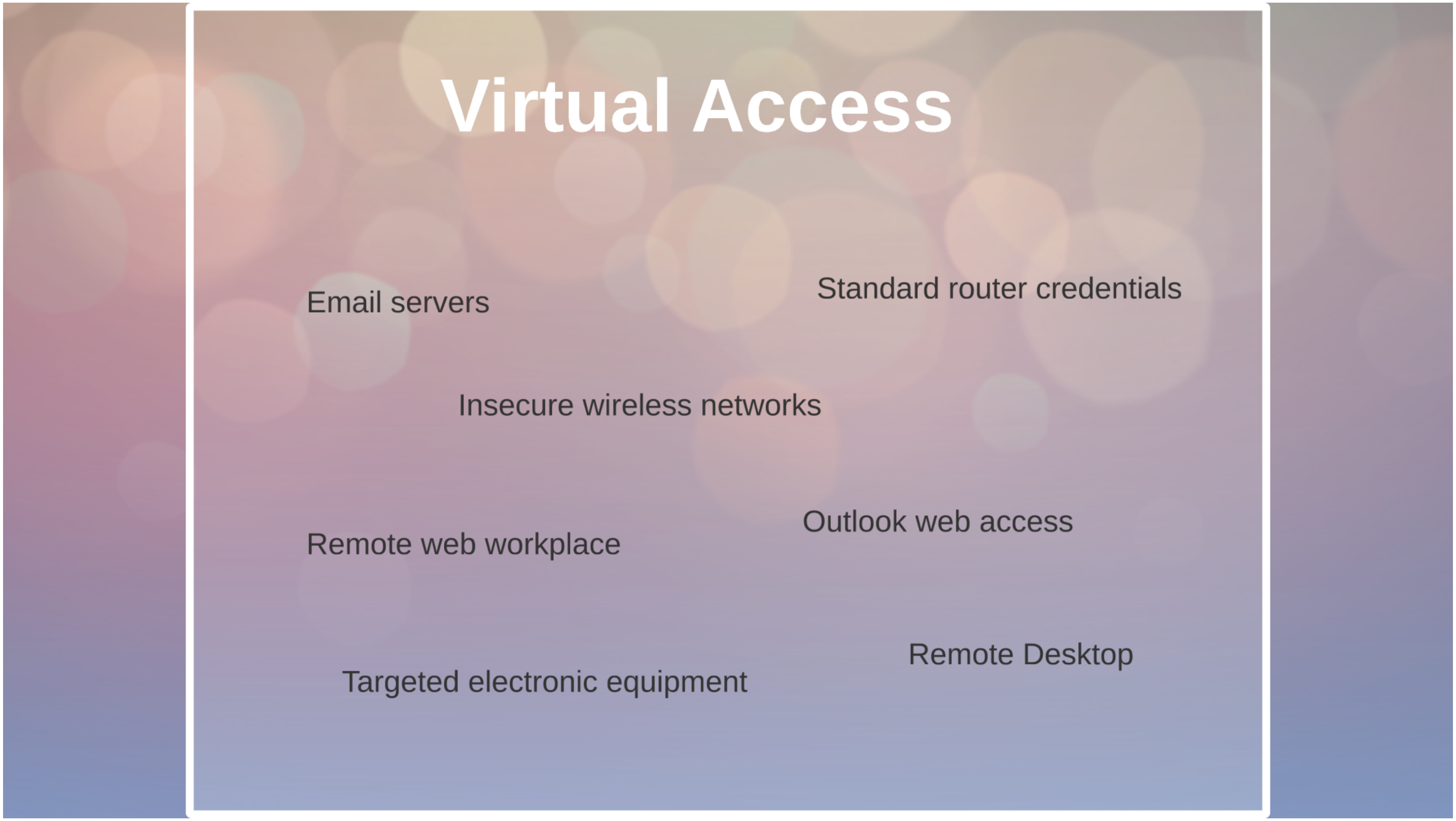
Standard router credentials

Insecure wireless networks

Remote web workplace

Outlook web access

Targeted electronic equipment



Virtual Access

Email servers

Standard router credentials

Insecure wireless networks

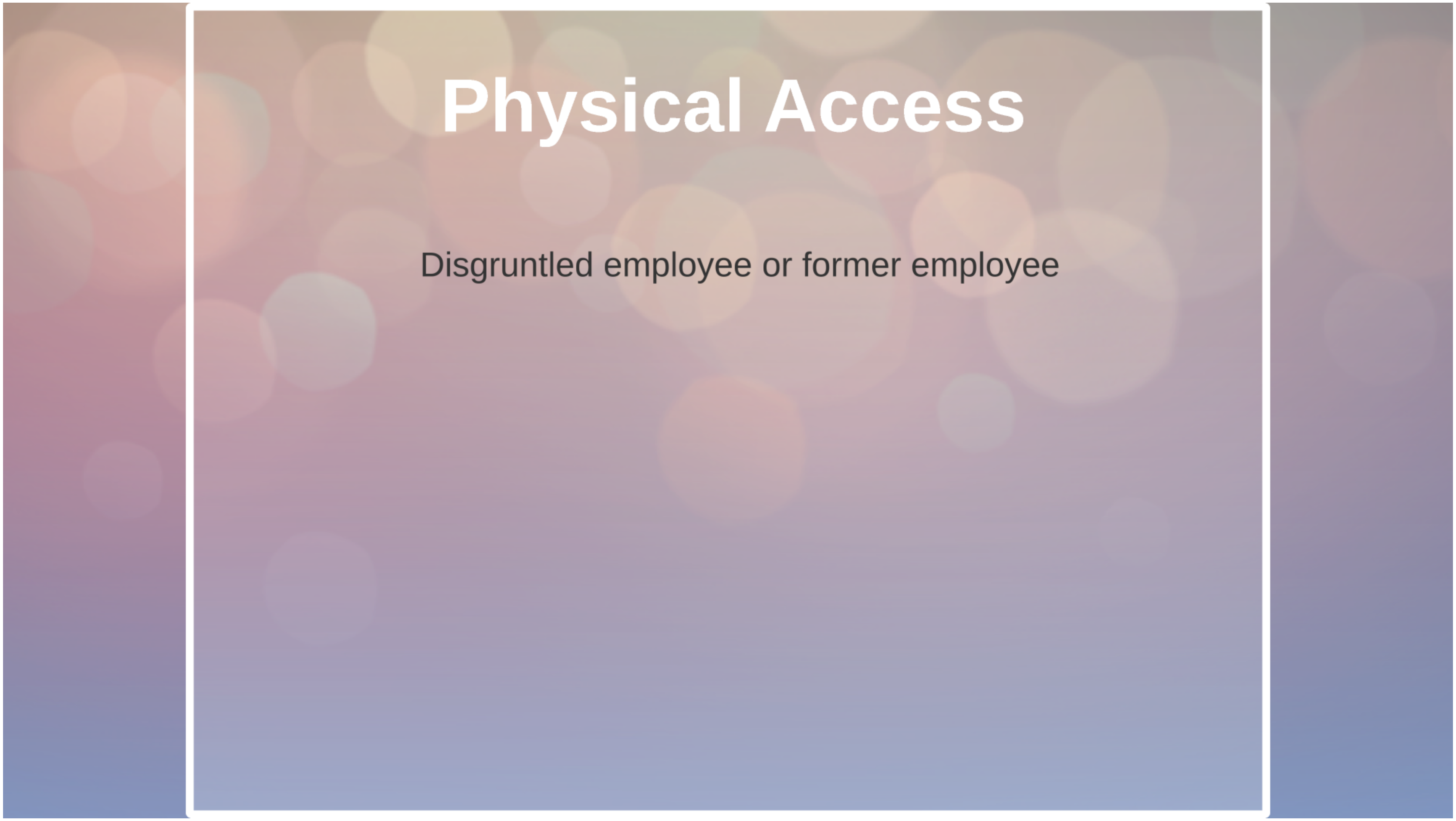
Remote web workplace

Outlook web access

Targeted electronic equipment

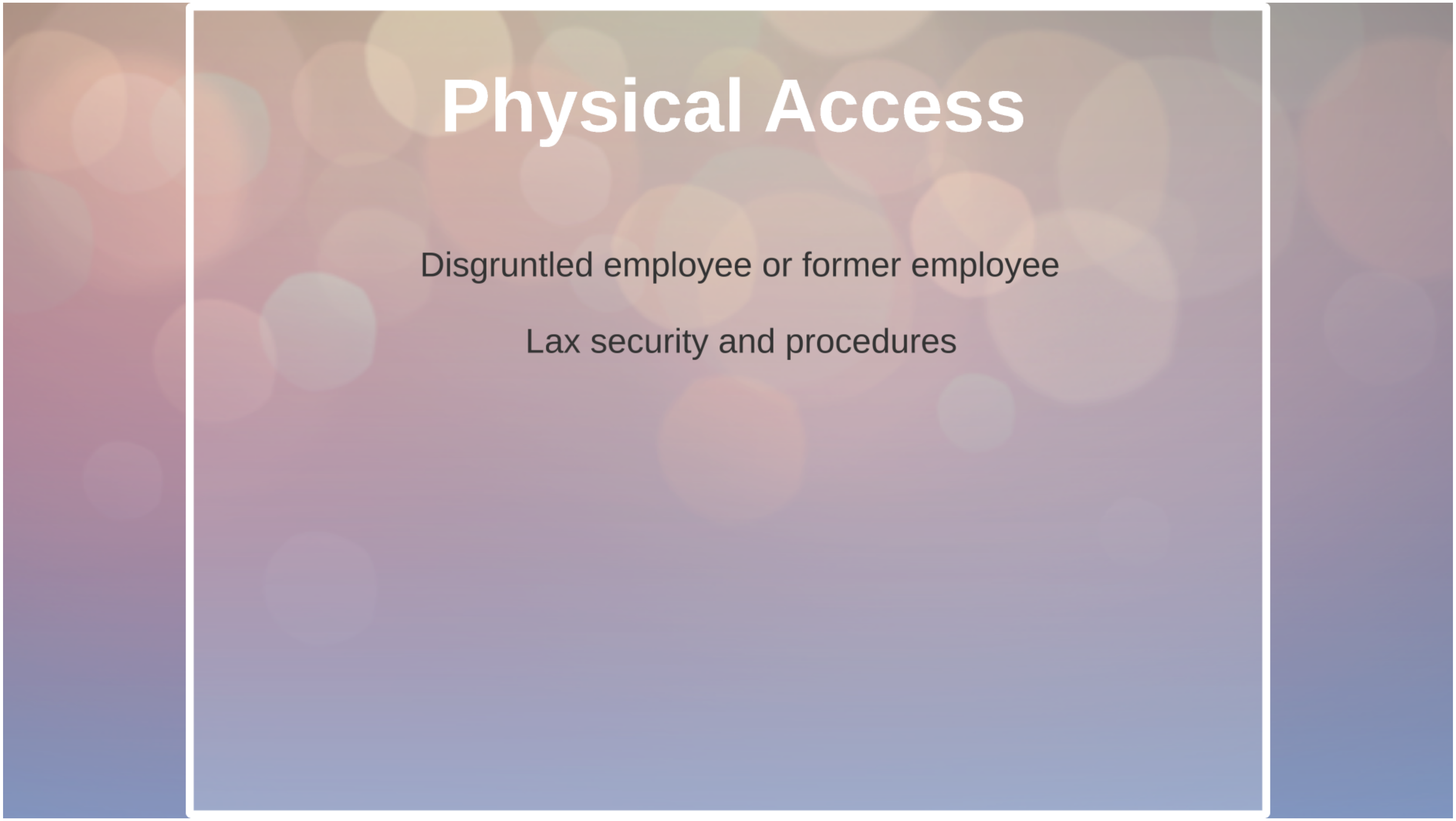
Remote Desktop

Physical Access



Physical Access

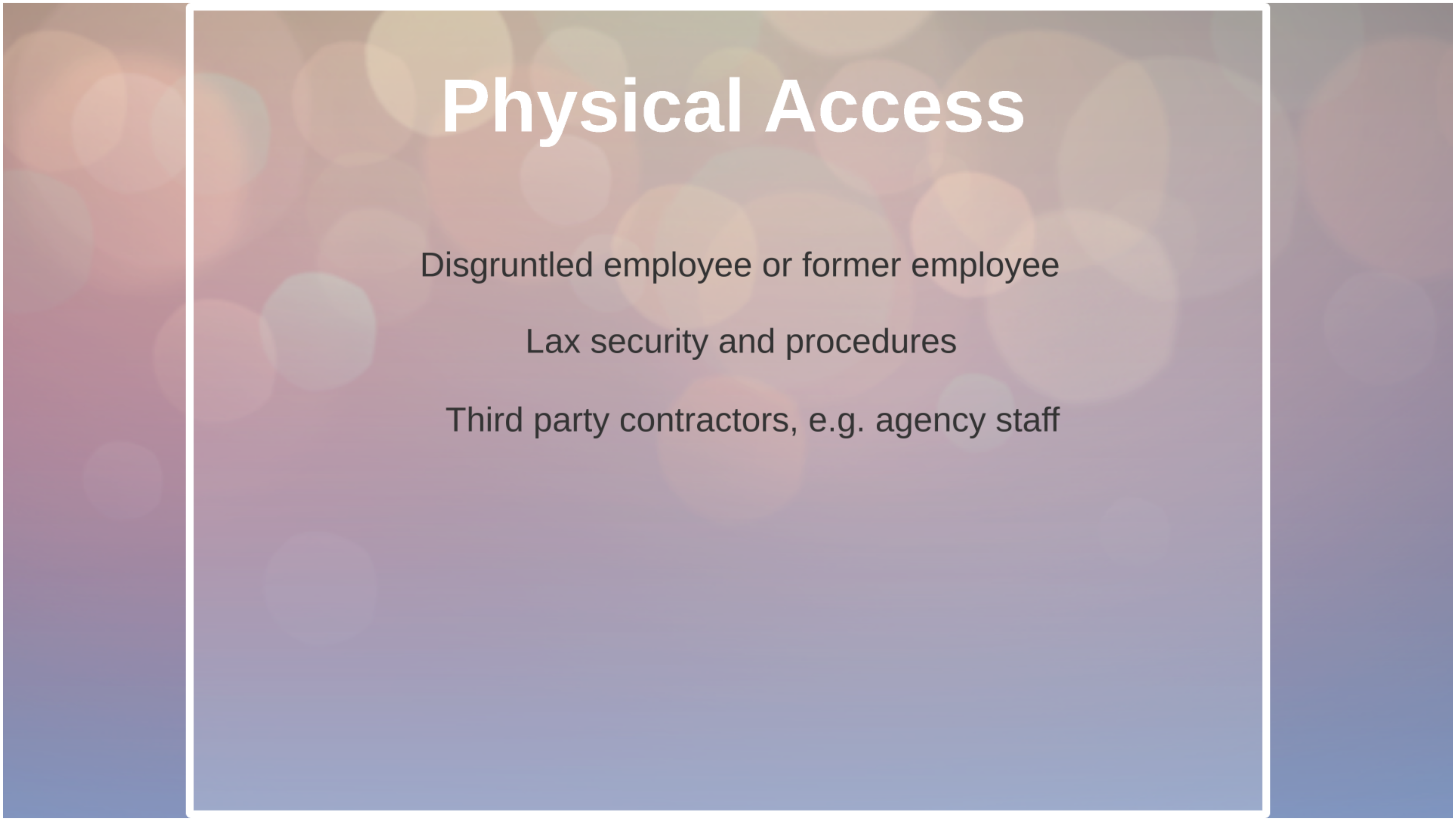
Disgruntled employee or former employee



Physical Access

Disgruntled employee or former employee

Lax security and procedures

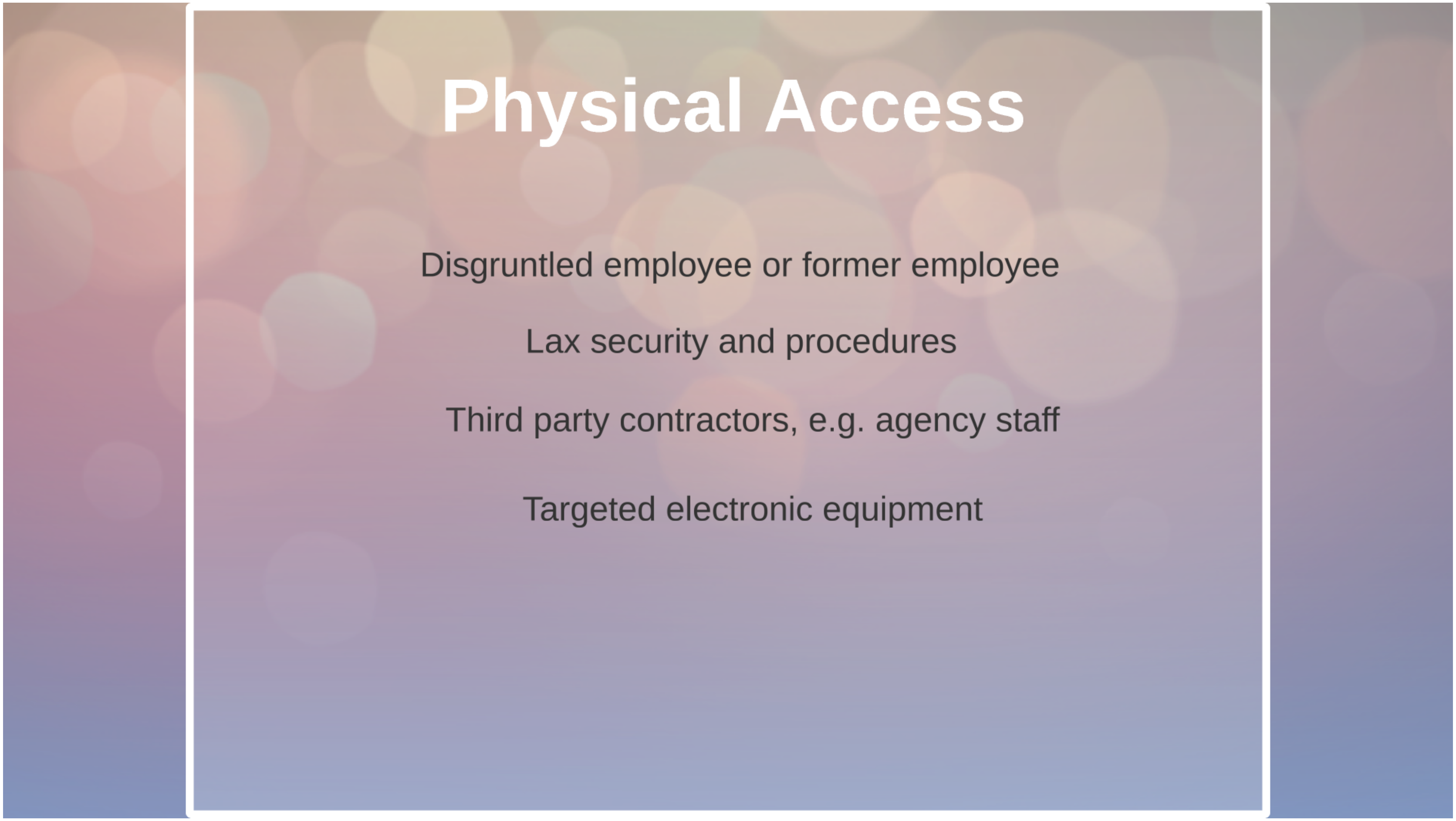


Physical Access

Disgruntled employee or former employee

Lax security and procedures

Third party contractors, e.g. agency staff



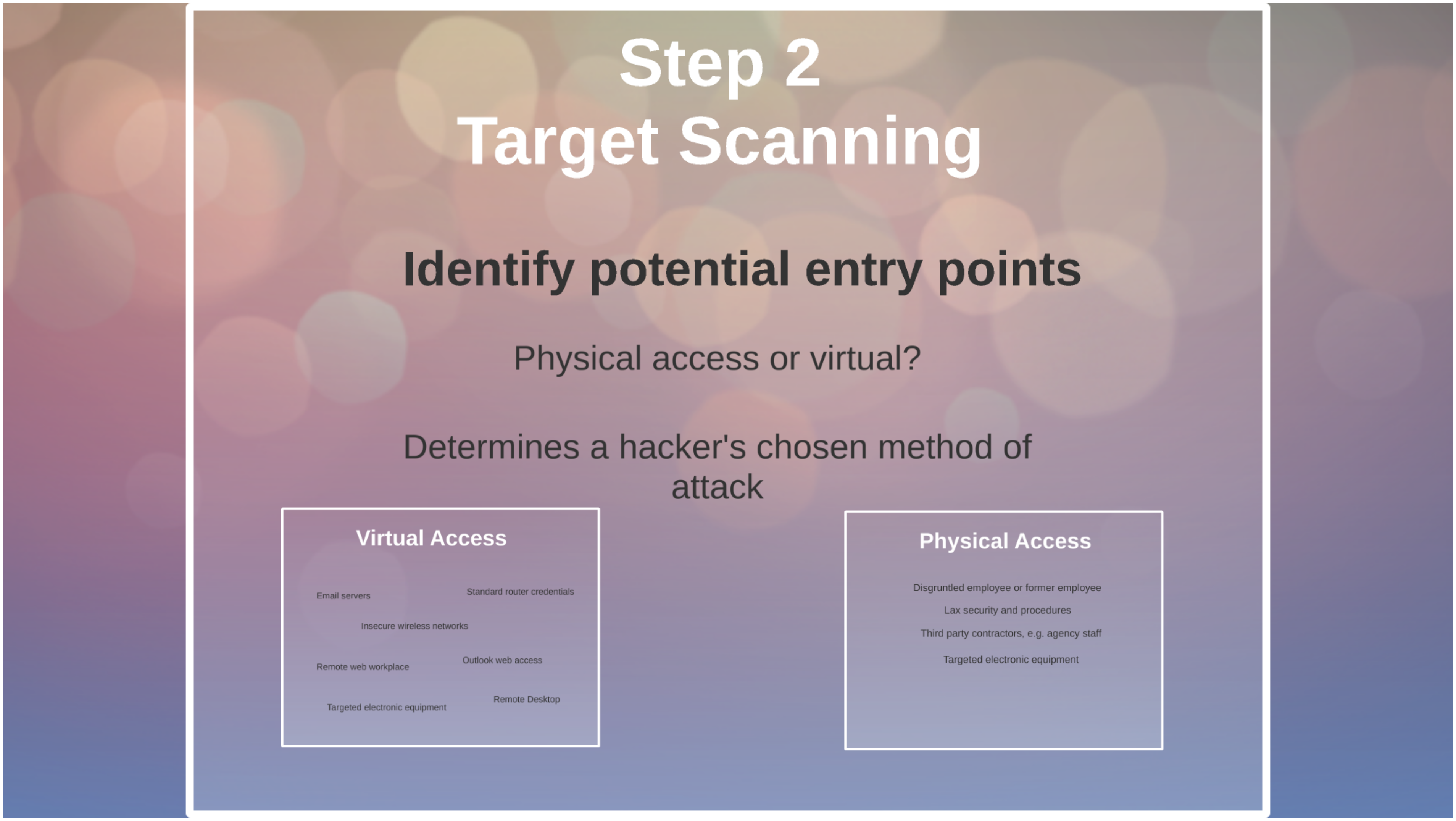
Physical Access

Disgruntled employee or former employee

Lax security and procedures

Third party contractors, e.g. agency staff

Targeted electronic equipment



Step 2
Target Scanning

Identify potential entry points

Physical access or virtual?

Determines a hacker's chosen method of attack

Virtual Access

Email servers

Standard router credentials

Insecure wireless networks

Remote web workplace

Outlook web access

Targeted electronic equipment

Remote Desktop

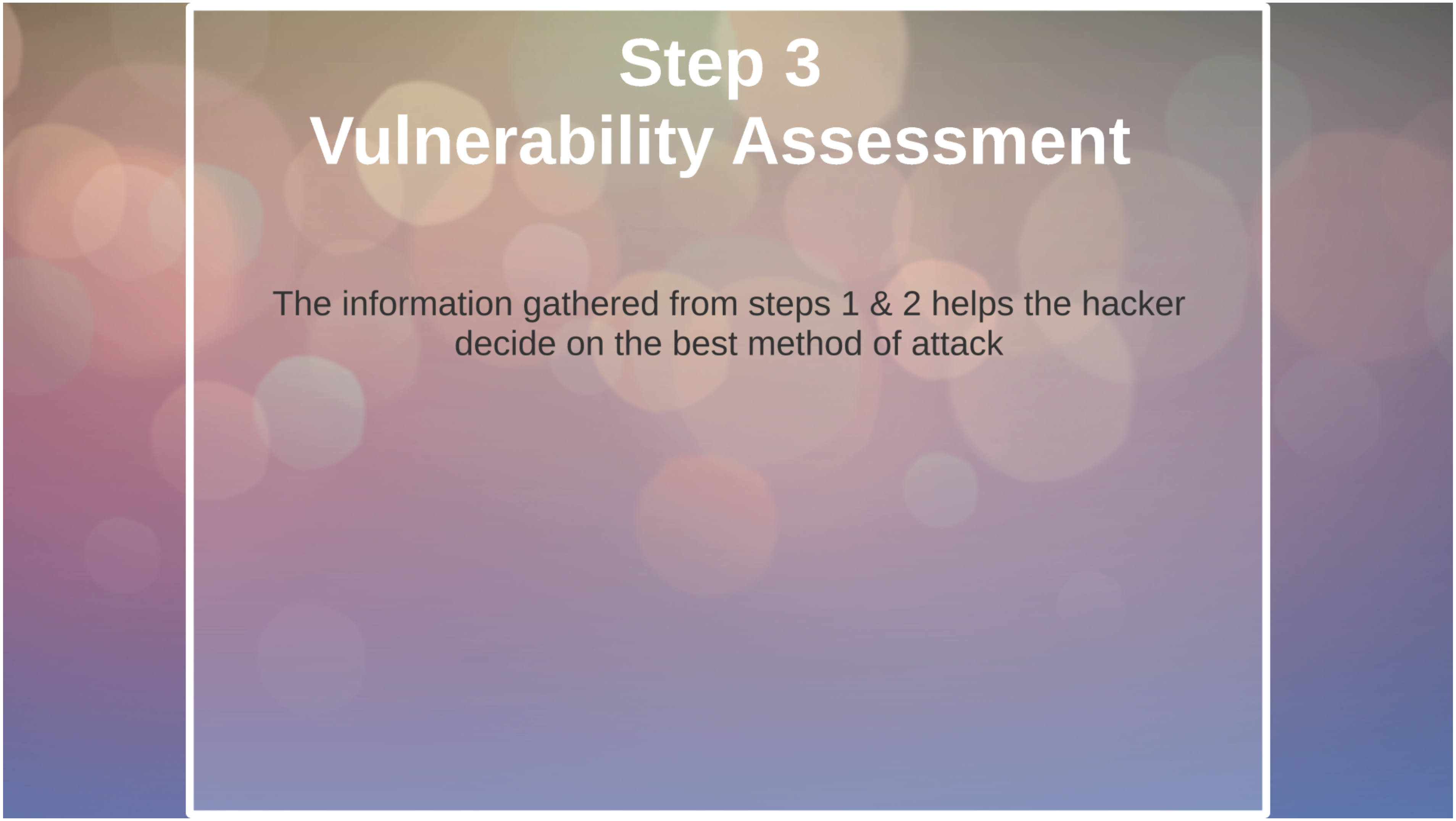
Physical Access

Disgruntled employee or former employee

Lax security and procedures

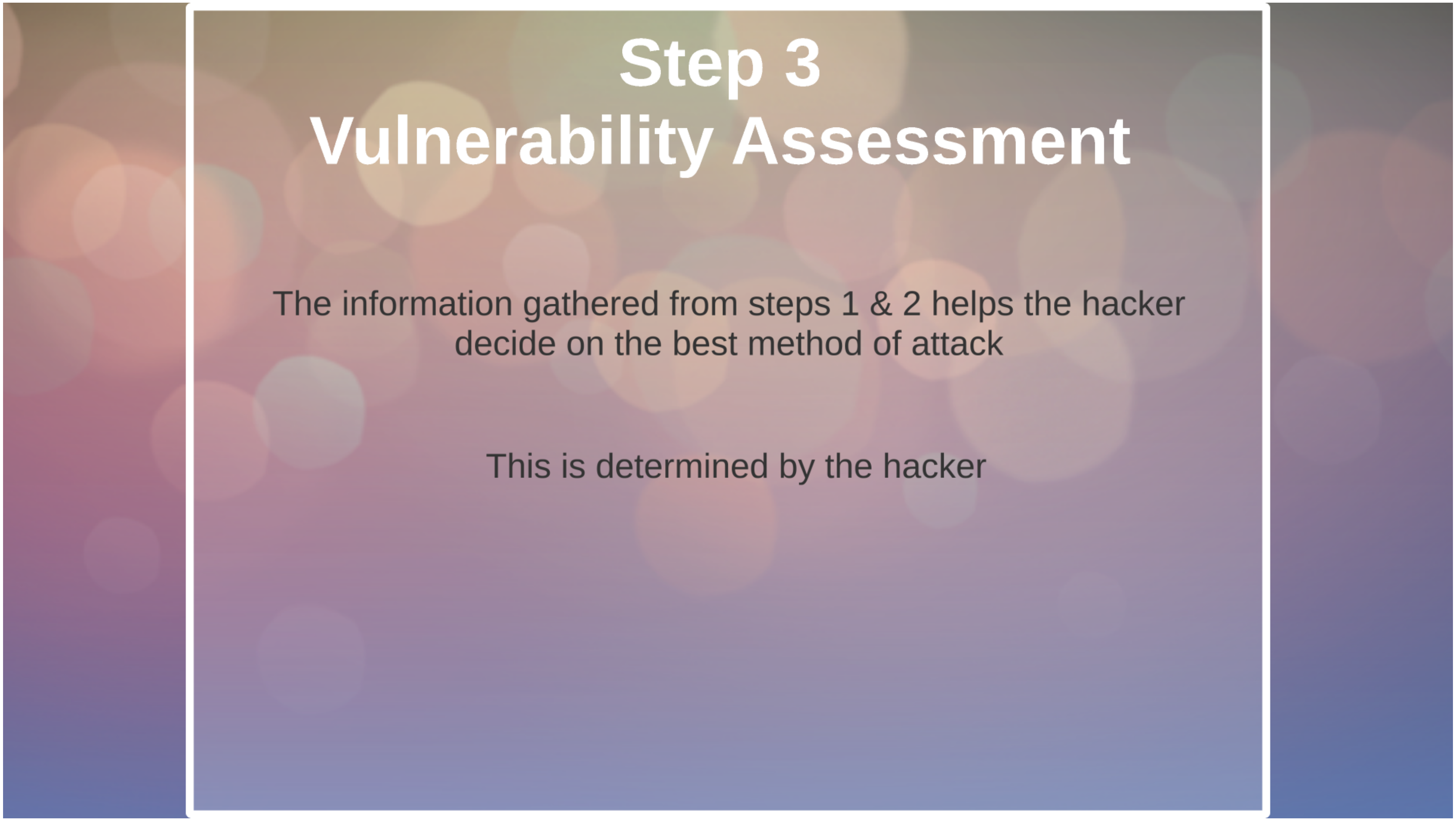
Third party contractors, e.g. agency staff

Targeted electronic equipment



Step 3
Vulnerability Assessment

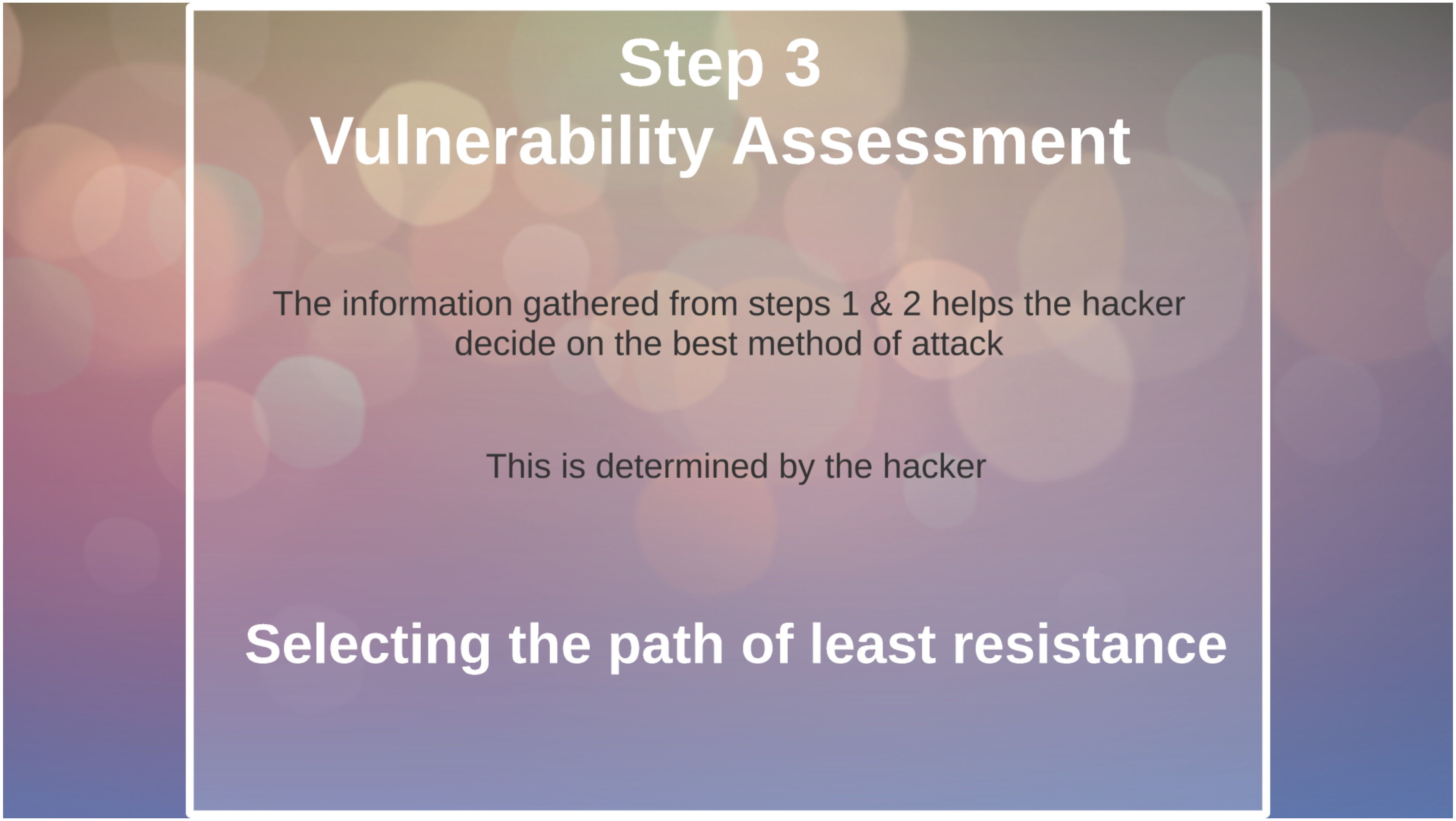
The information gathered from steps 1 & 2 helps the hacker decide on the best method of attack



Step 3
Vulnerability Assessment

The information gathered from steps 1 & 2 helps the hacker decide on the best method of attack

This is determined by the hacker



Step 3
Vulnerability Assessment

The information gathered from steps 1 & 2 helps the hacker decide on the best method of attack

This is determined by the hacker

Selecting the path of least resistance

Step 4
Exploiting the weakness

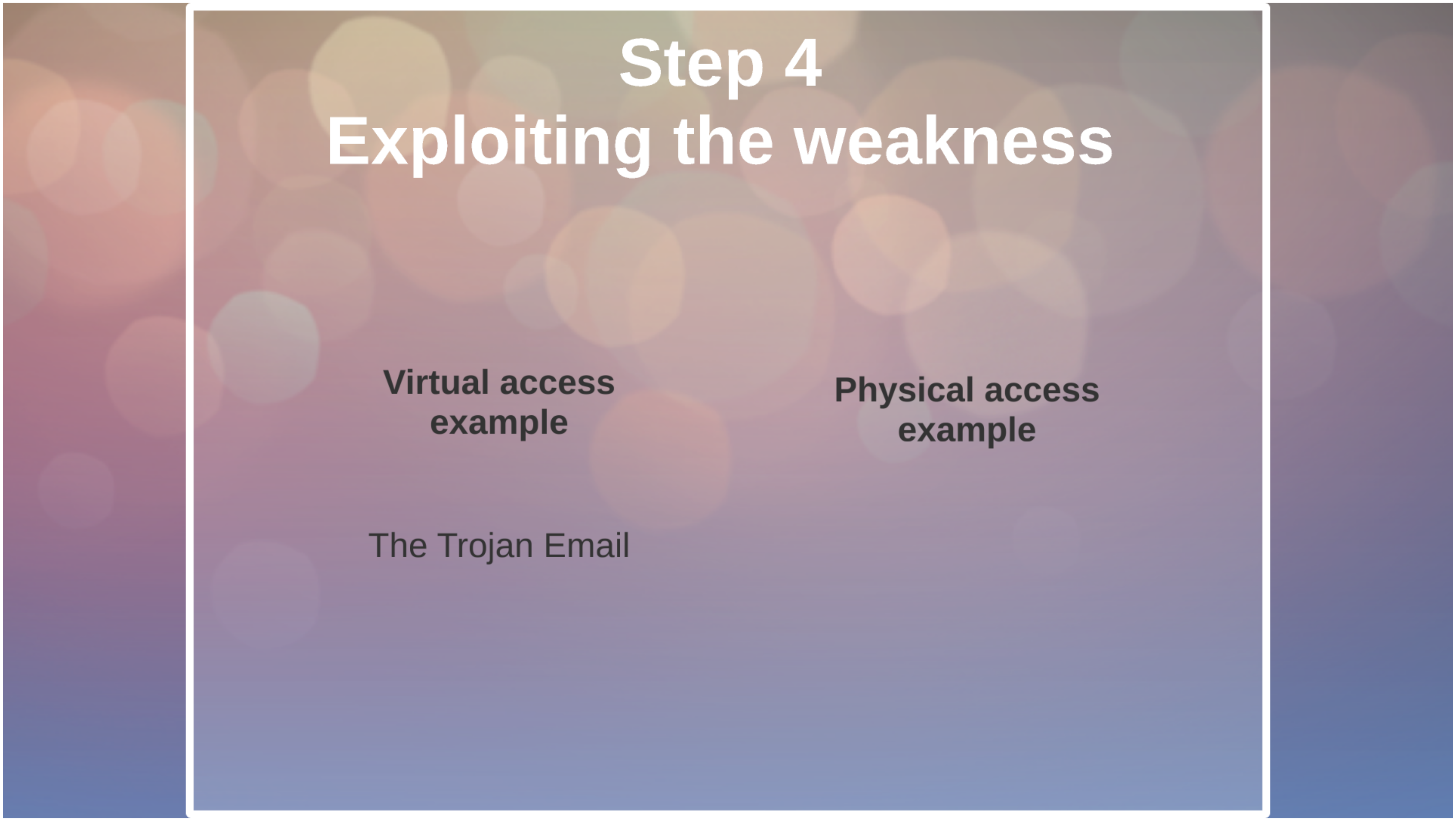
Step 4
Exploiting the weakness

Virtual access
example

Step 4
Exploiting the weakness

Virtual access example

The Trojan Email

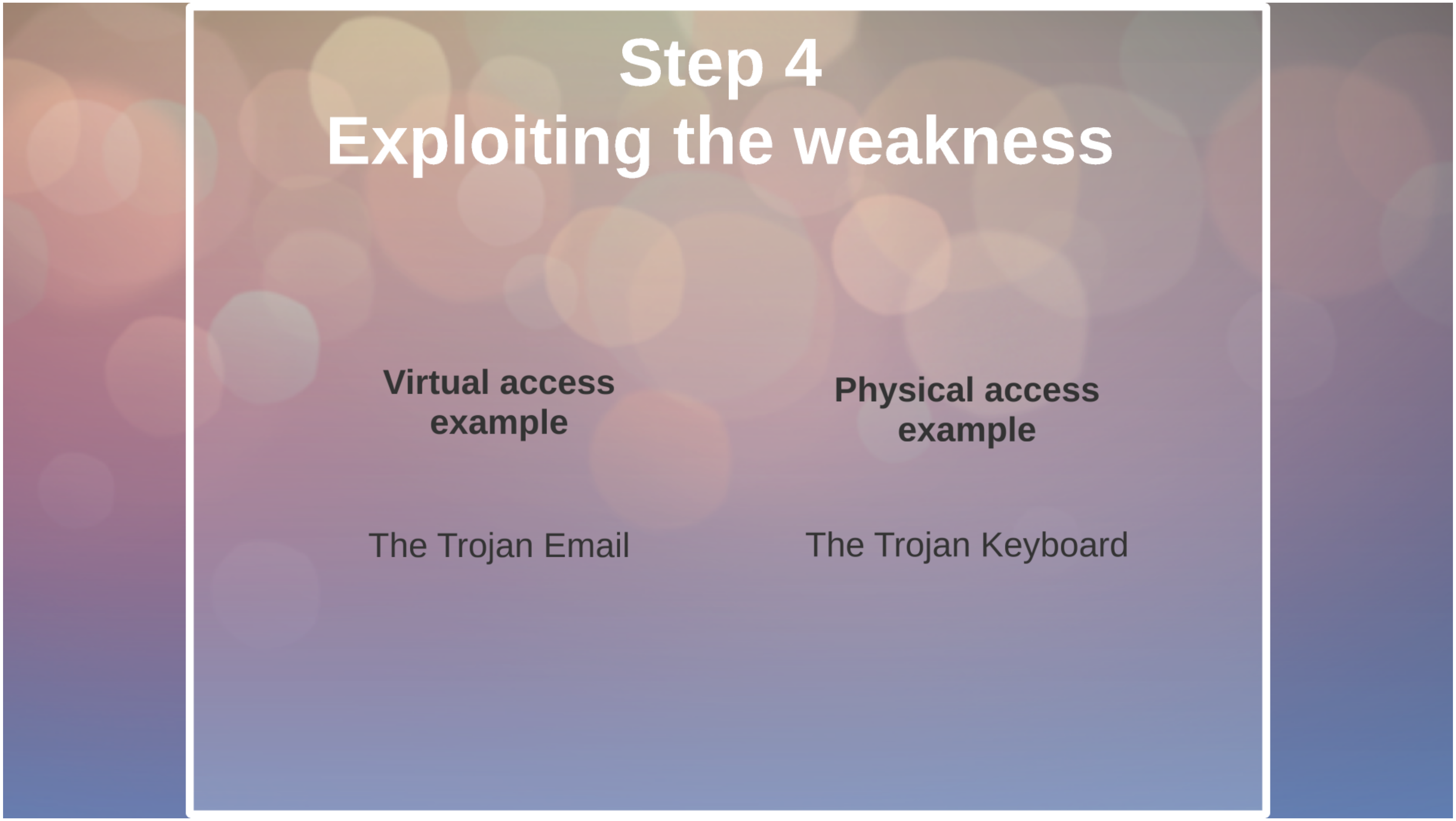


Step 4
Exploiting the weakness

Virtual access example

The Trojan Email

Physical access example



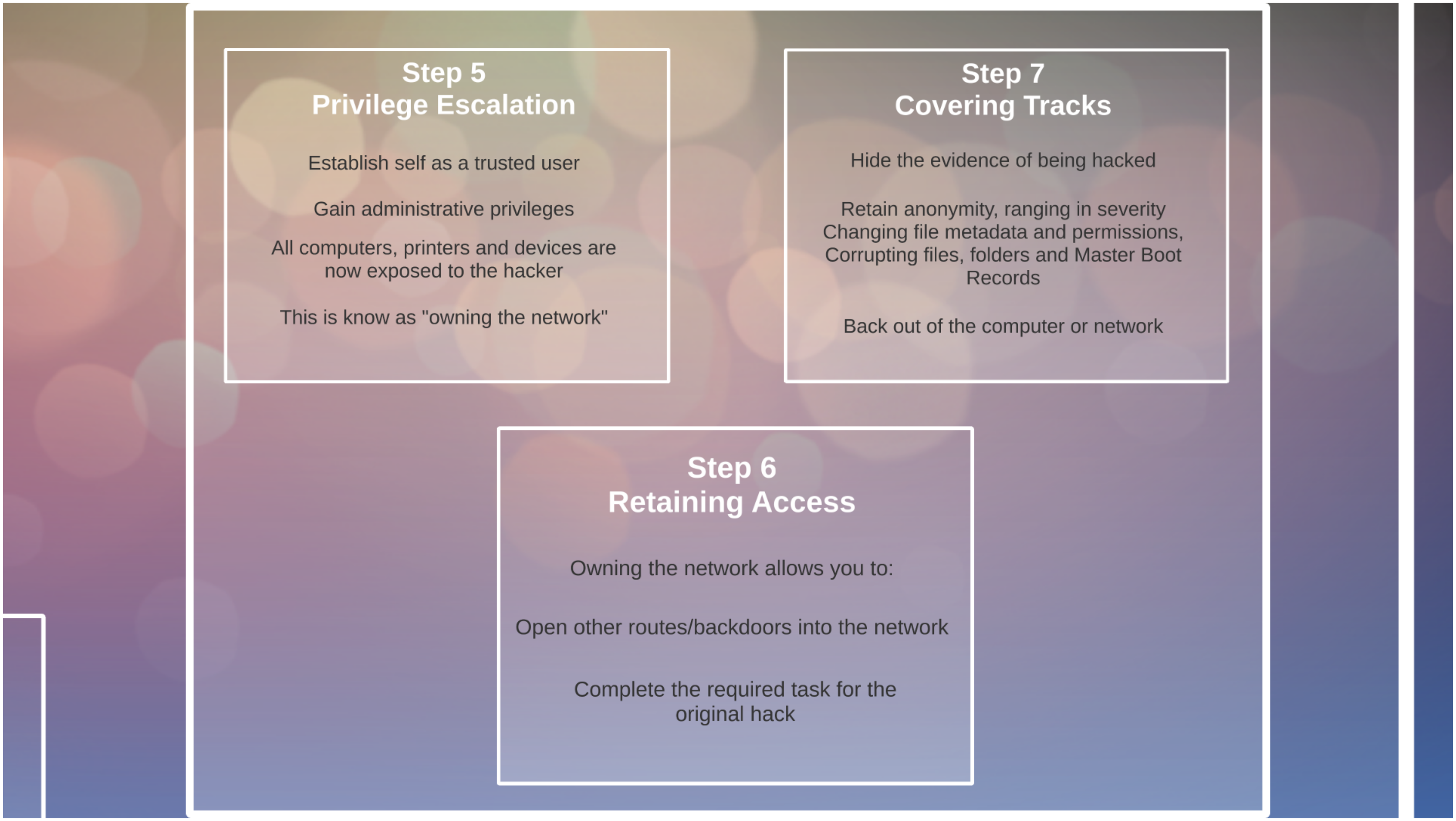
Step 4
Exploiting the weakness

Virtual access example

The Trojan Email

Physical access example

The Trojan Keyboard



Step 5
Privilege Escalation

Establish self as a trusted user

Gain administrative privileges

All computers, printers and devices are now exposed to the hacker

This is know as "owning the network"

Step 6
Retaining Access

Owning the network allows you to:

Open other routes/backdoors into the network

Complete the required task for the original hack

Step 7
Covering Tracks

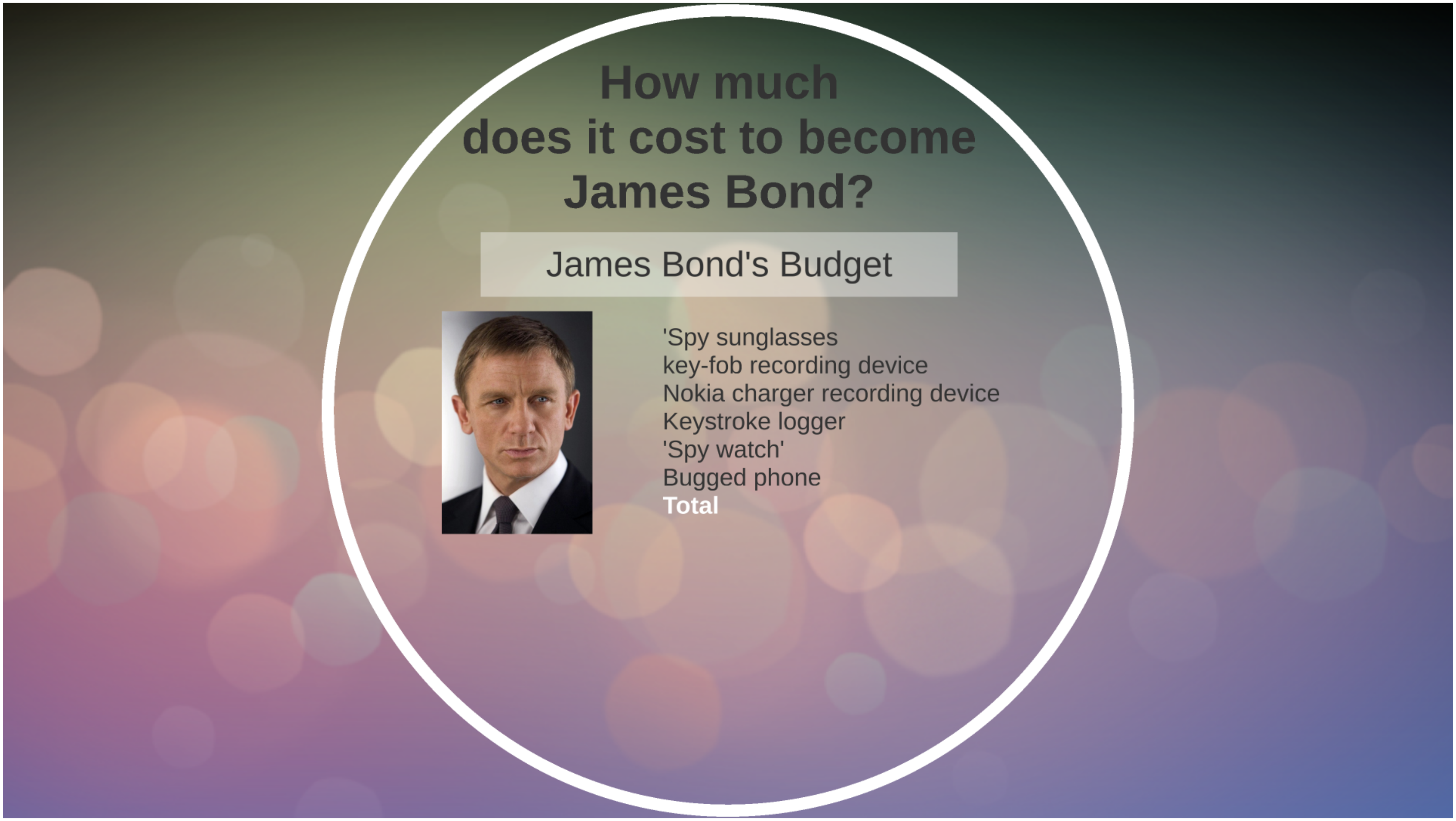
Hide the evidence of being hacked

Retain anonymity, ranging in severity
Changing file metadata and permissions,
Corrupting files, folders and Master Boot Records

Back out of the computer or network

How much does it cost to become James Bond?

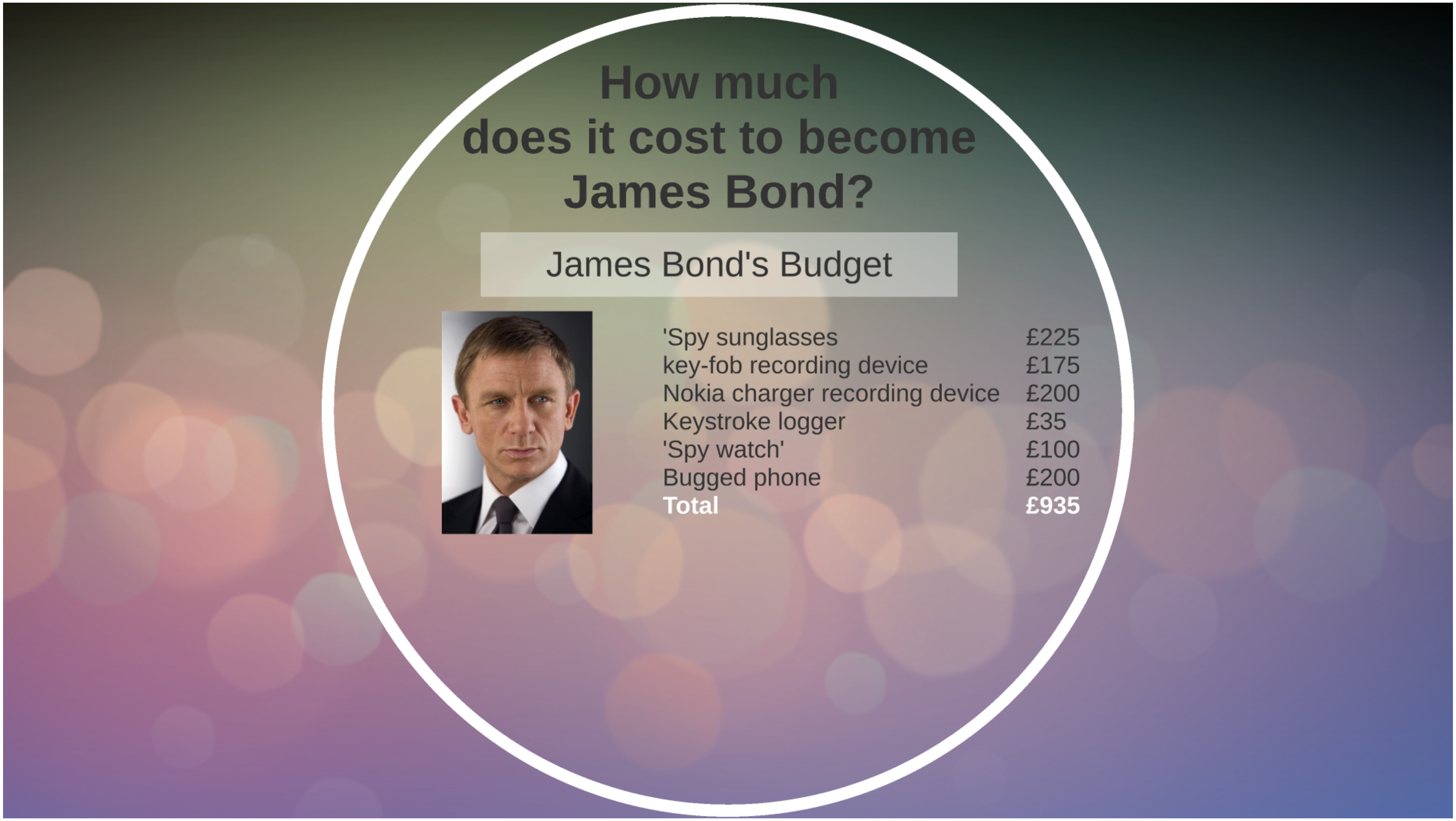
James Bond's Budget



How much does it cost to become James Bond?

James Bond's Budget

'Spy sunglasses
key-fob recording device
Nokia charger recording device
Keystroke logger
'Spy watch'
Bugged phone
Total



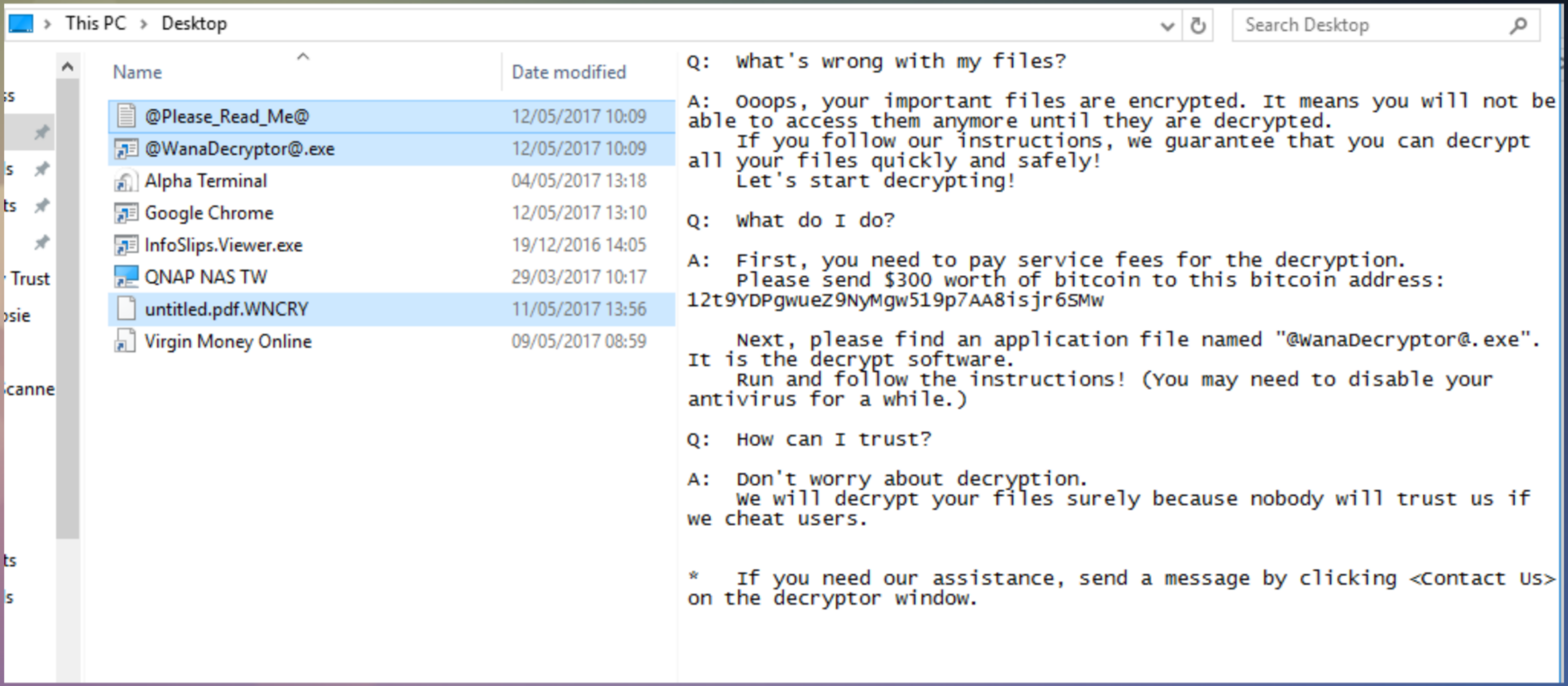
How much does it cost to become James Bond?

James Bond's Budget

'Spy sunglasses	£225
key-fob recording device	£175
Nokia charger recording device	£200
Keystroke logger	£35
'Spy watch'	£100
Bugged phone	£200
Total	**£935**

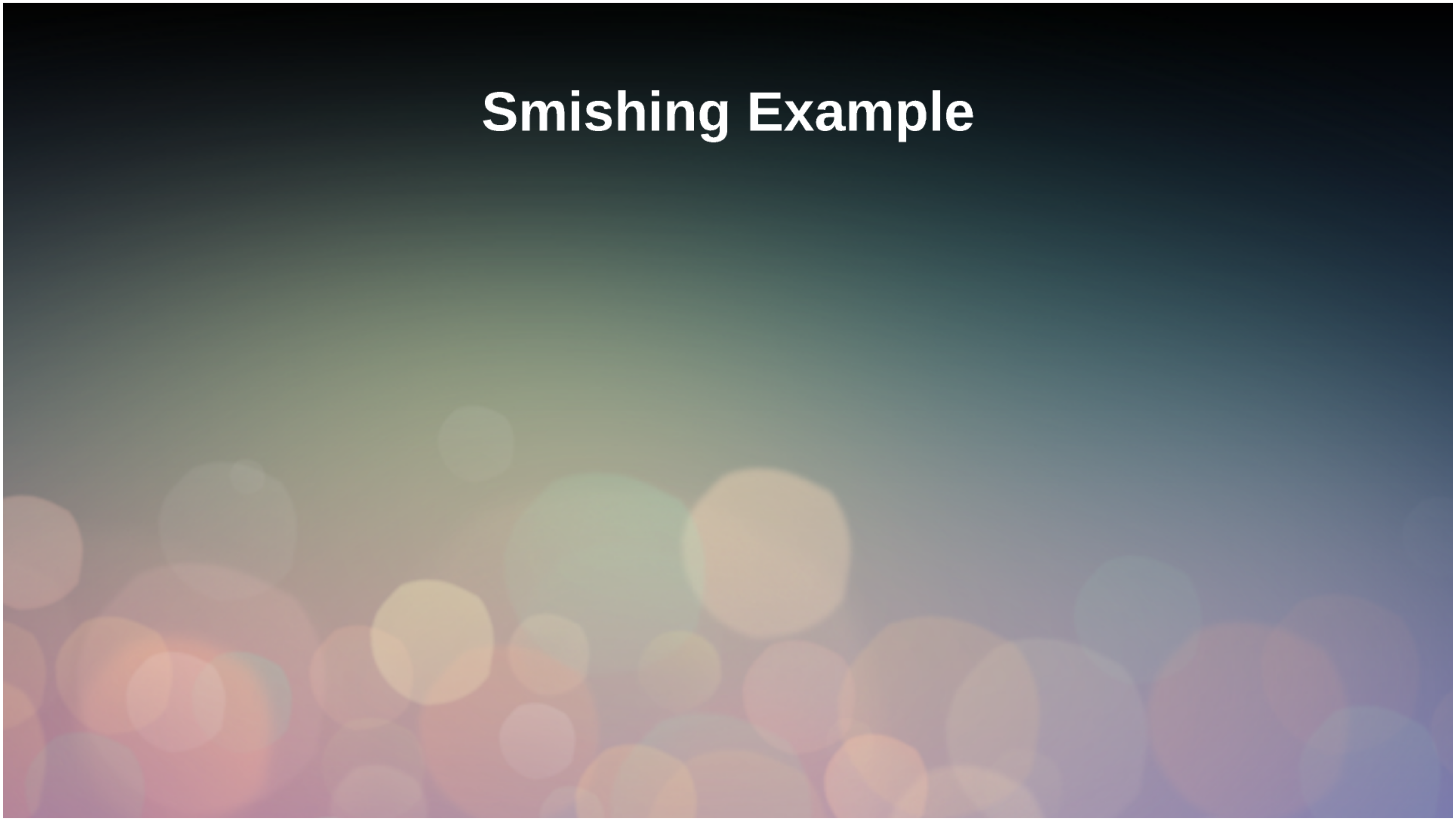
Wanacrypt Ransomware Example

Wanacrypt Ransomware Example



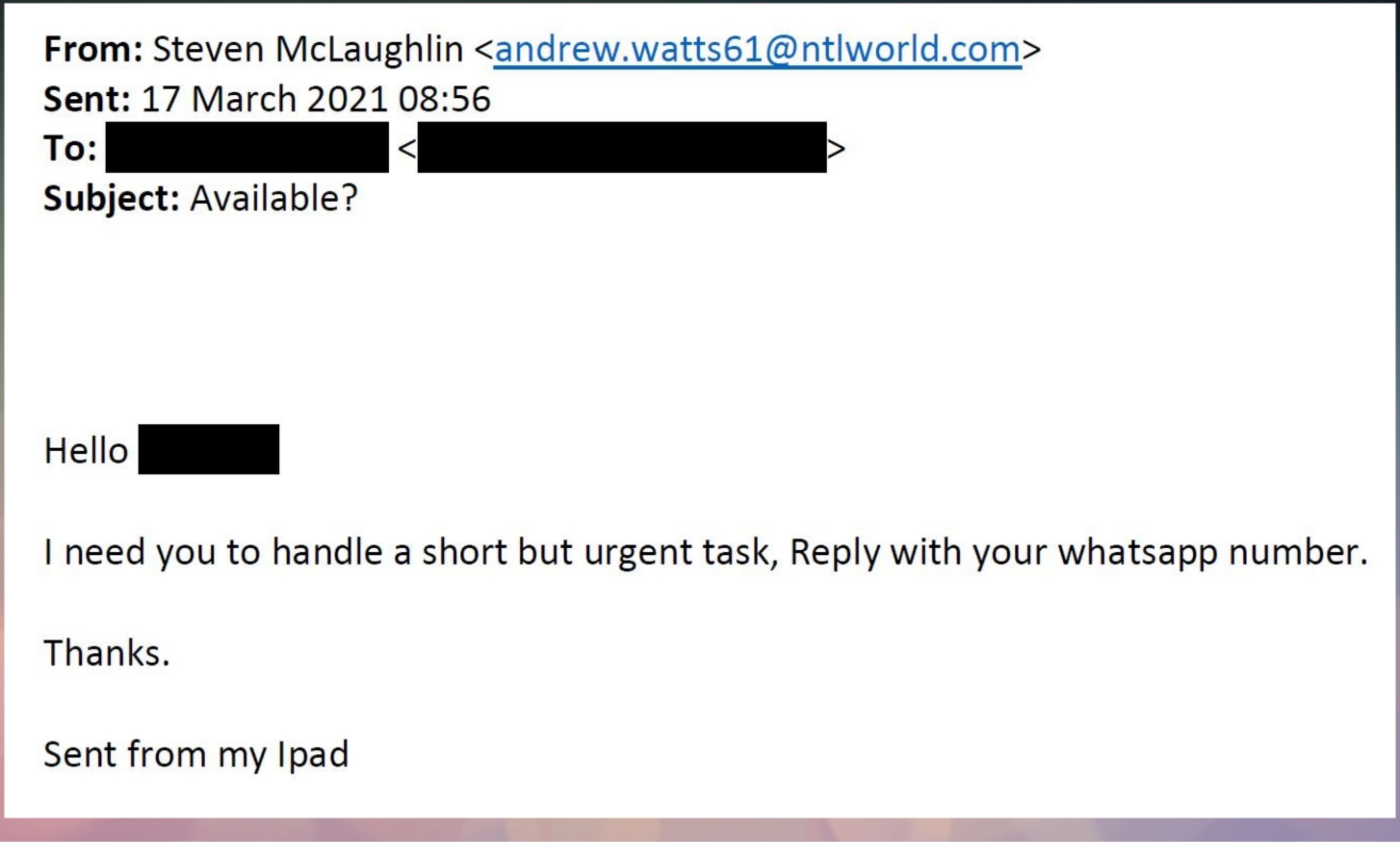
Name	Date modified
@Please_Read_Me@	12/05/2017 10:09
@WanaDecryptor@.exe	12/05/2017 10:09
Alpha Terminal	04/05/2017 13:18
Google Chrome	12/05/2017 13:10
InfoSlips.Viewer.exe	19/12/2016 14:05
QNAP NAS TW	29/03/2017 10:17
untitled.pdf.WNCRY	11/05/2017 13:56
Virgin Money Online	09/05/2017 08:59

```
Q:  What's wrong with my files?

A:  Ooops, your important files are encrypted. It means you will not be
able to access them anymore until they are decrypted.
    If you follow our instructions, we guarantee that you can decrypt
all your files quickly and safely!
    Let's start decrypting!

Q:  What do I do?

A:  First, you need to pay service fees for the decryption.
    Please send $300 worth of bitcoin to this bitcoin address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

    Next, please find an application file named "@WanaDecryptor@.exe".
It is the decrypt software.
    Run and follow the instructions! (You may need to disable your
antivirus for a while.)

Q:  How can I trust?

A:  Don't worry about decryption.
    We will decrypt your files surely because nobody will trust us if
we cheat users.


*   If you need our assistance, send a message by clicking <Contact Us>
on the decryptor window.
```



Smishing Example

Smishing Example



From: Steven McLaughlin <andrew.watts61@ntlworld.com>
Sent: 17 March 2021 08:56
To: [redacted] <[redacted]>
Subject: Available?

Hello [redacted]

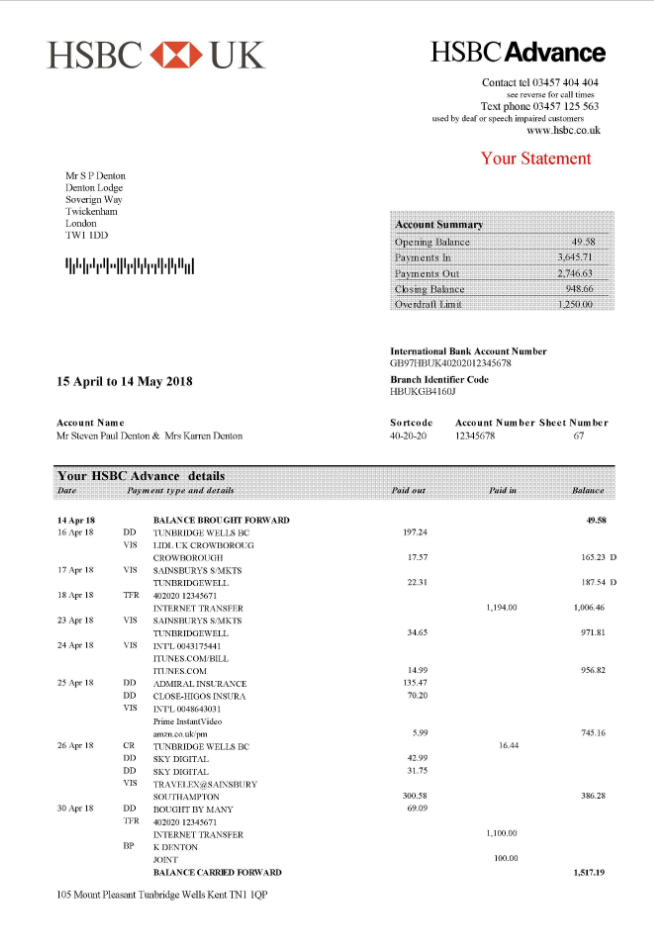
I need you to handle a short but urgent task, Reply with your whatsapp number.

Thanks.

Sent from my Ipad

Genuine v Fake Bank Statement

Genuine v Fake Bank Statement



HSBC UK

HSBC Advance

Contact tel 03457 404 404
see reverse for call times
Text phone 03457 125 563
used by deaf or speech impaired customers
www.hsbc.co.uk

Your Statement

Mr S P Denton
Denton Lodge
Soverign Way
Twickenham
London
TW1 1DD

Account Summary	
Opening Balance	49.58
Payments In	3,645.71
Payments Out	2,746.63
Closing Balance	948.66
Overdraft Limit	1,250.00

International Bank Account Number
GB97HBUK40202012345678

Branch Identifier Code
HBUKGB4160J

15 April to 14 May 2018

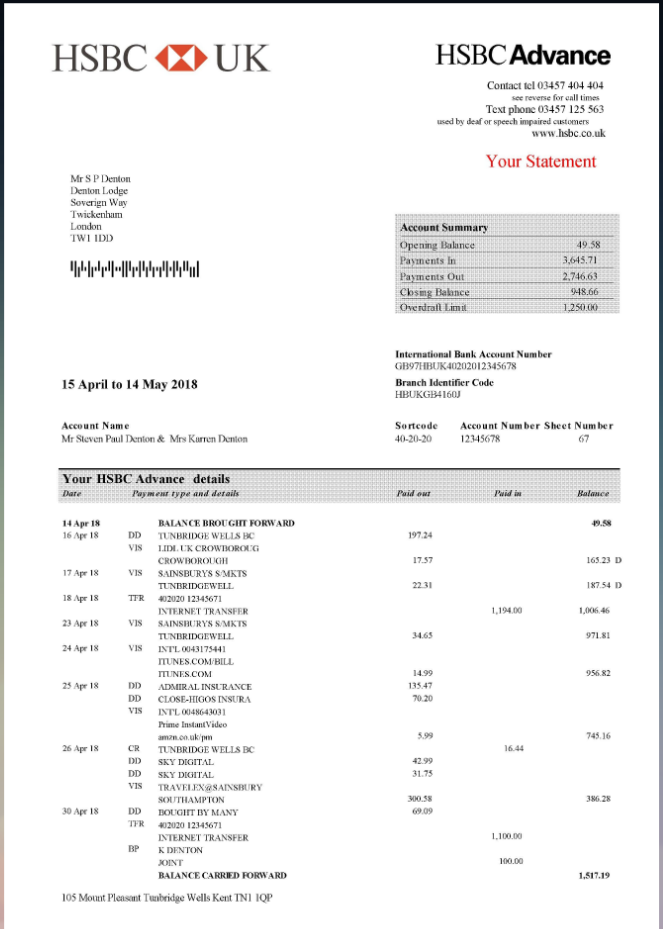
Account Name	Sortcode	Account Number	Sheet Number
Mr Steven Paul Denton & Mrs Karren Denton	40-20-20	12345678	67

Your HSBC Advance details

Date	*Payment type and details*		*Paid out*	*Paid in*	*Balance*
14 Apr 18		**BALANCE BROUGHT FORWARD**			**49.58**
16 Apr 18	DD	TUNBRIDGE WELLS BC	197.24		
	VIS	LIDL UK CROWBOROUG			
		CROWBOROUGH	17.57		165.23 D
17 Apr 18	VIS	SAINSBURYS S/MKTS			
		TUNBRIDGEWELL	22.31		187.54 D
18 Apr 18	TFR	402020 12345671			
		INTERNET TRANSFER		1,194.00	1,006.46
23 Apr 18	VIS	SAINSBURYS S/MKTS			
		TUNBRIDGEWELL	34.65		971.81
24 Apr 18	VIS	INT'L 0043175441			
		ITUNES.COM/BILL			
		ITUNES.COM	14.99		956.82
25 Apr 18	DD	ADMIRAL INSURANCE	135.47		
	DD	CLOSE-HIGOS INSURA	70.20		
	VIS	INT'L 0048643031			
		Prime InstantVideo			
		amzn.co.uk/pm	5.99		745.16
26 Apr 18	CR	TUNBRIDGE WELLS BC		16.44	
	DD	SKY DIGITAL	42.99		
	DD	SKY DIGITAL	31.75		
	VIS	TRAVELEX@SAINSBURY			
		SOUTHAMPTON	300.58		386.28
30 Apr 18	DD	BOUGHT BY MANY	69.09		
	TFR	402020 12345671			
		INTERNET TRANSFER		1,100.00	
	BP	K DENTON			
		JOINT		100.00	
		BALANCE CARRIED FORWARD			**1,517.19**

105 Mount Pleasant Tunbridge Wells Kent TN1 1QP

Genuine v Fake Bank Statement



HSBC UK

HSBC Advance

Contact tel 03457 404 404
see reverse for call times
Text phone 03457 125 563
used by deaf or speech impaired customers
www.hsbc.co.uk

Your Statement

Mr S P Denton
Denton Lodge
Soverign Way
Twickenham
London
TW1 1DD

Account Summary	
Opening Balance	49.58
Payments In	3,645.71
Payments Out	2,746.63
Closing Balance	948.66
Overdraft Limit	1,250.00

International Bank Account Number
GB97HBUK40202012345678

Branch Identifier Code
HBUKGB4160J

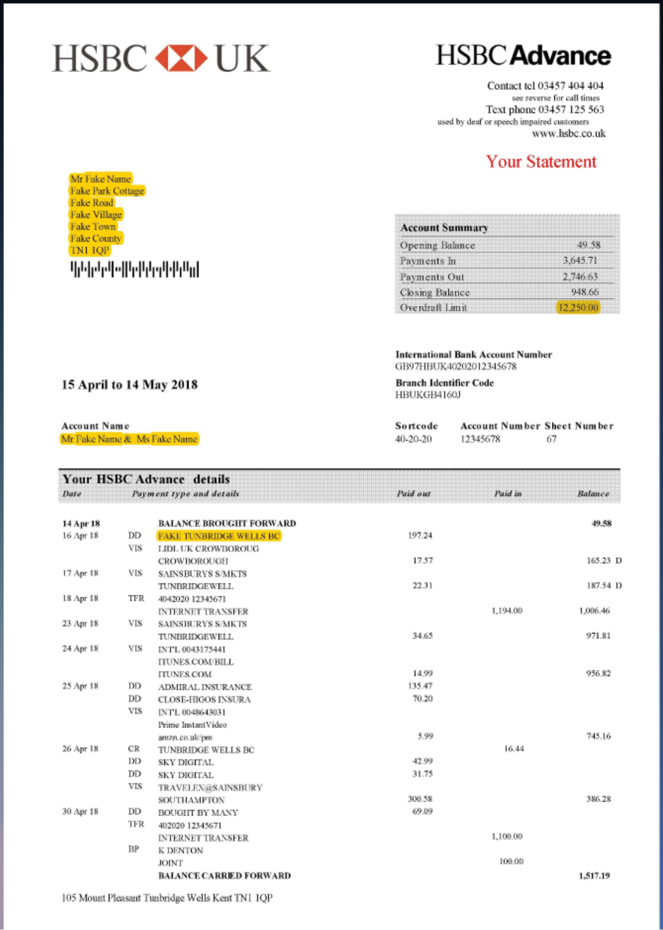
15 April to 14 May 2018

Account Name	Sortcode	Account Number	Sheet Number
Mr Steven Paul Denton & Mrs Karren Denton	40-20-20	12345678	67

Your HSBC Advance details

Date	Payment type and details		Paid out	Paid in	Balance
14 Apr 18		**BALANCE BROUGHT FORWARD**			**49.58**
16 Apr 18	DD	TUNBRIDGE WELLS BC	197.24		
	VIS	LIDL UK CROWBOROUG			
		CROWBOROUGH	17.57		165.23 D
17 Apr 18	VIS	SAINSBURYS S/MKTS			
		TUNBRIDGEWELL	22.31		187.54 D
18 Apr 18	TFR	402020 12345671			
		INTERNET TRANSFER		1,194.00	1,006.46
23 Apr 18	VIS	SAINSBURYS S/MKTS			
		TUNBRIDGEWELL	34.65		971.81
24 Apr 18	VIS	INT'L 0043175441			
		ITUNES.COM/BILL			
		ITUNES.COM	14.99		956.82
25 Apr 18	DD	ADMIRAL INSURANCE	135.47		
	DD	CLOSE-HIGOS INSURA	70.20		
	VIS	INT'L 0048643031			
		Prime InstantVideo			
		amzn.co.uk/pm	5.99		745.16
26 Apr 18	CR	TUNBRIDGE WELLS BC		16.44	
	DD	SKY DIGITAL	42.99		
	DD	SKY DIGITAL	31.75		
	VIS	TRAVELEX@SAINSBURY			
		SOUTHAMPTON	300.58		386.28
30 Apr 18	DD	BOUGHT BY MANY	69.09		
	TFR	402020 12345671			
		INTERNET TRANSFER		1,100.00	
	BP	K DENTON			
		JOINT		100.00	
		BALANCE CARRIED FORWARD			**1,517.19**

105 Mount Pleasant Tunbridge Wells Kent TN1 1QP



HSBC UK

HSBC Advance

Contact tel 03457 404 404
see reverse for call times
Text phone 03457 125 563
used by deaf or speech impaired customers
www.hsbc.co.uk

Your Statement

Mr Fake Name
Fake Park Cottage
Fake Road
Fake Village
Fake Town
Fake County
TN1 1QP

Account Summary	
Opening Balance	49.58
Payments In	3,645.71
Payments Out	2,746.63
Closing Balance	948.66
Overdraft Limit	12,250.00

International Bank Account Number
GB97HBUK40202012345678

Branch Identifier Code
HBUKGB4160J

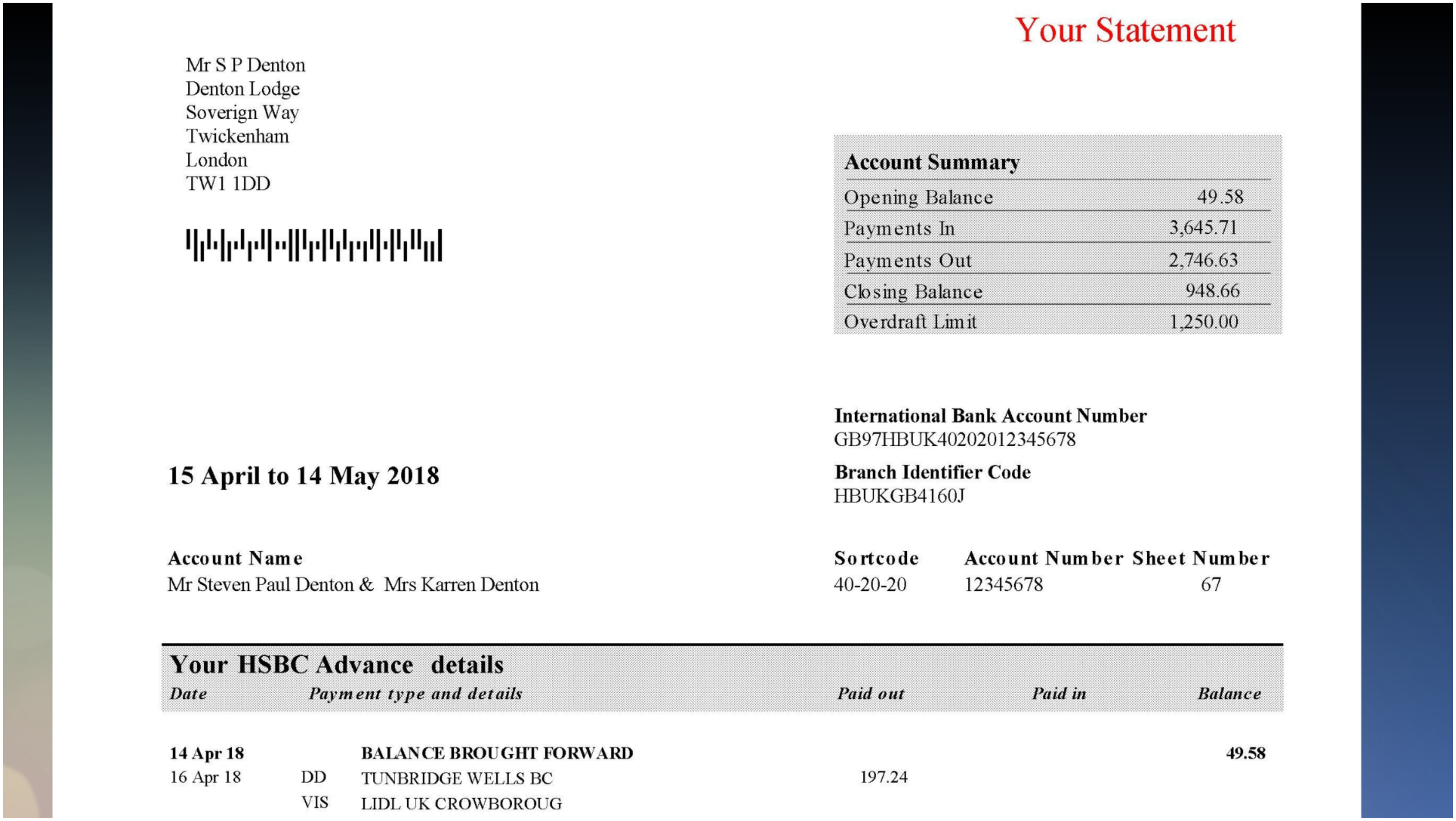
15 April to 14 May 2018

Account Name	Sortcode	Account Number	Sheet Number
Mr Fake Name & Ms Fake Name	40-20-20	12345678	67

Your HSBC Advance details

Date	Payment type and details		Paid out	Paid in	Balance
14 Apr 18		**BALANCE BROUGHT FORWARD**			**49.58**
16 Apr 18	DD	FAKE TUNBRIDGE WELLS BC	197.24		
	VIS	LIDL UK CROWBOROUG			
		CROWBOROUGH	17.57		165.23 D
17 Apr 18	VIS	SAINSBURYS S/MKTS			
		TUNBRIDGEWELL	22.31		187.54 D
18 Apr 18	TFR	4042020 12345671			
		INTERNET TRANSFER		1,194.00	1,006.46
23 Apr 18	VIS	SAINSBURYS S/MKTS			
		TUNBRIDGEWELL	34.65		971.81
24 Apr 18	VIS	INT'L 0043175441			
		ITUNES.COM/BILL			
		ITUNES.COM	14.99		956.82
25 Apr 18	DD	ADMIRAL INSURANCE	135.47		
	DD	CLOSE-HIGOS INSURA	70.20		
	VIS	INT'L 0048643031			
		Prime InstantVideo			
		amzn.co.uk/pm	5.99		745.16
26 Apr 18	CR	TUNBRIDGE WELLS BC		16.44	
	DD	SKY DIGITAL	42.99		
	DD	SKY DIGITAL	31.75		
	VIS	TRAVELEX@SAINSBURY			
		SOUTHAMPTON	300.58		386.28
30 Apr 18	DD	BOUGHT BY MANY	69.09		
	TFR	402020 12345671			
		INTERNET TRANSFER		1,100.00	
	BP	K DENTON			
		JOINT		100.00	
		BALANCE CARRIED FORWARD			**1,517.19**

105 Mount Pleasant Tunbridge Wells Kent TN1 1QP



Your Statement

Mr S P Denton
Denton Lodge
Soverign Way
Twickenham
London
TW1 1DD

Account Summary	
Opening Balance	49.58
Payments In	3,645.71
Payments Out	2,746.63
Closing Balance	948.66
Overdraft Limit	1,250.00

International Bank Account Number
GB97HBUK40202012345678

Branch Identifier Code
HBUKGB4160J

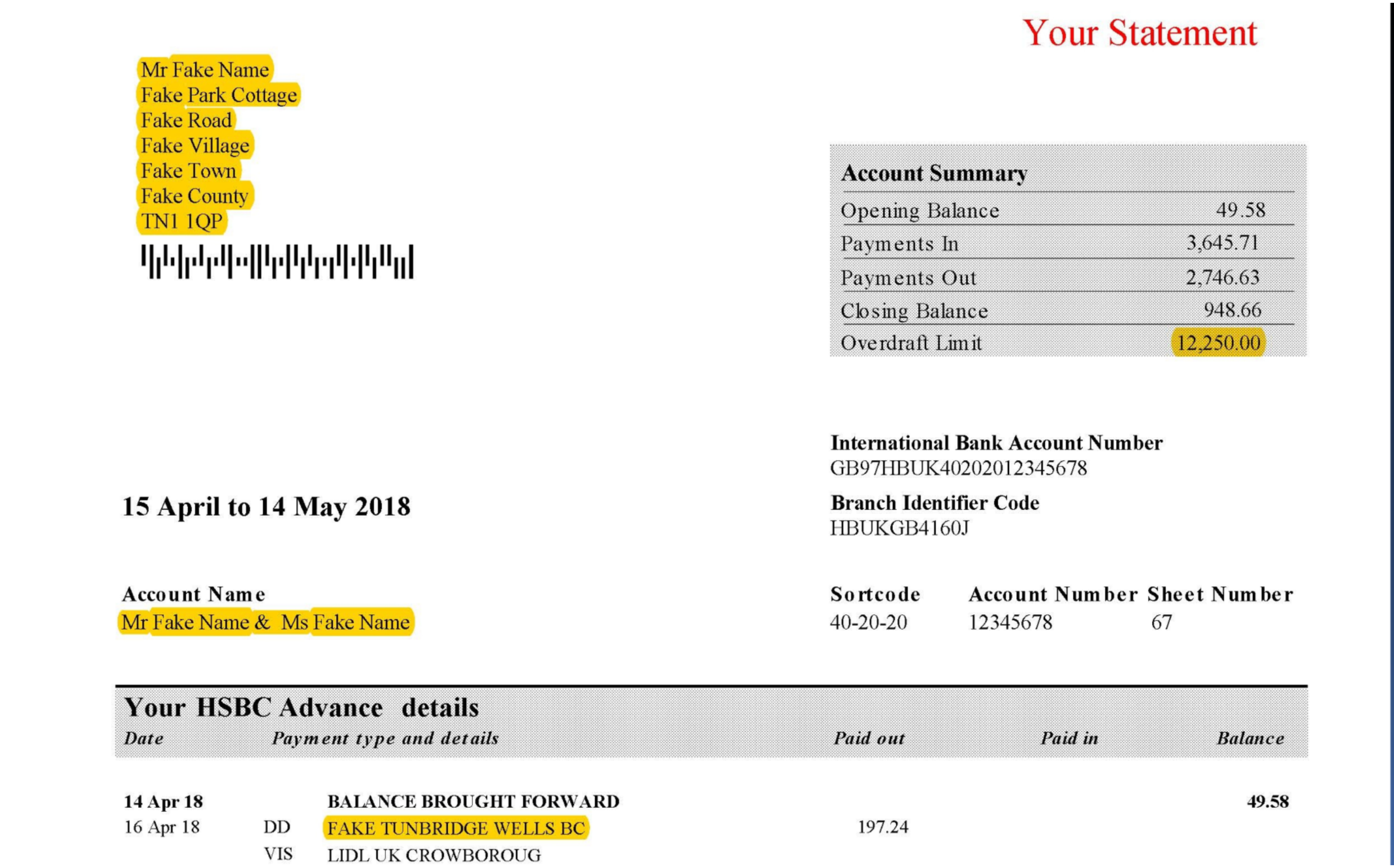
15 April to 14 May 2018

Account Name
Mr Steven Paul Denton & Mrs Karren Denton

Sortcode	Account Number	Sheet Number
40-20-20	12345678	67

Your HSBC Advance details

Date		*Payment type and details*	*Paid out*	*Paid in*	*Balance*
14 Apr 18		**BALANCE BROUGHT FORWARD**			**49.58**
16 Apr 18	DD	TUNBRIDGE WELLS BC	197.24		
	VIS	LIDL UK CROWBOROUG			



Your Statement

Mr Fake Name
Fake Park Cottage
Fake Road
Fake Village
Fake Town
Fake County
TN1 1QP

Account Summary	
Opening Balance	49.58
Payments In	3,645.71
Payments Out	2,746.63
Closing Balance	948.66
Overdraft Limit	12,250.00

International Bank Account Number
GB97HBUK40202012345678

Branch Identifier Code
HBUKGB4160J

15 April to 14 May 2018

Account Name
Mr Fake Name & Ms Fake Name

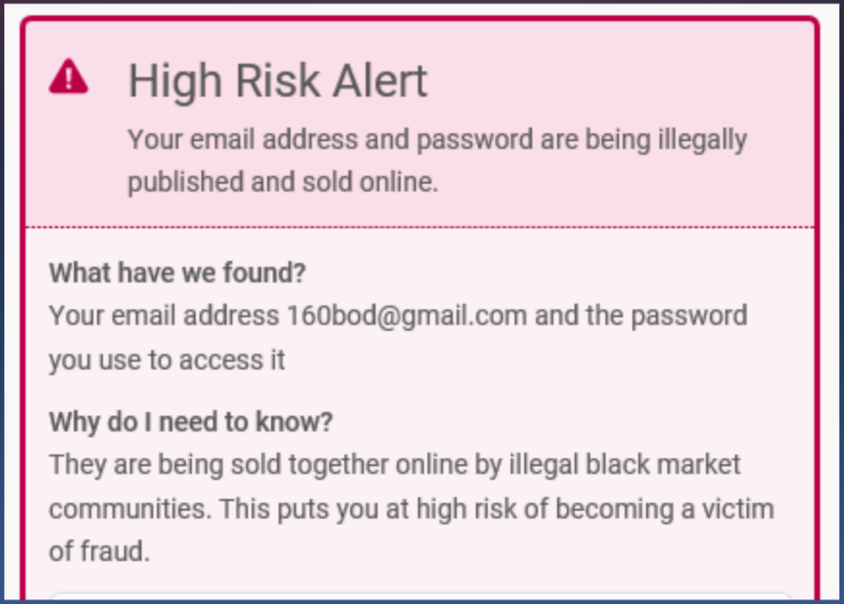
Sortcode	Account Number	Sheet Number
40-20-20	12345678	67

Your HSBC Advance details

Date		*Payment type and details*	*Paid out*	*Paid in*	*Balance*
14 Apr 18		**BALANCE BROUGHT FORWARD**			**49.58**
16 Apr 18	DD	FAKE TUNBRIDGE WELLS BC	197.24		
	VIS	LIDL UK CROWBOROUG			

" IT HAPPENS TO THE BEST OF US "

" IT HAPPENS TO THE BEST OF US "



⚠ High Risk Alert

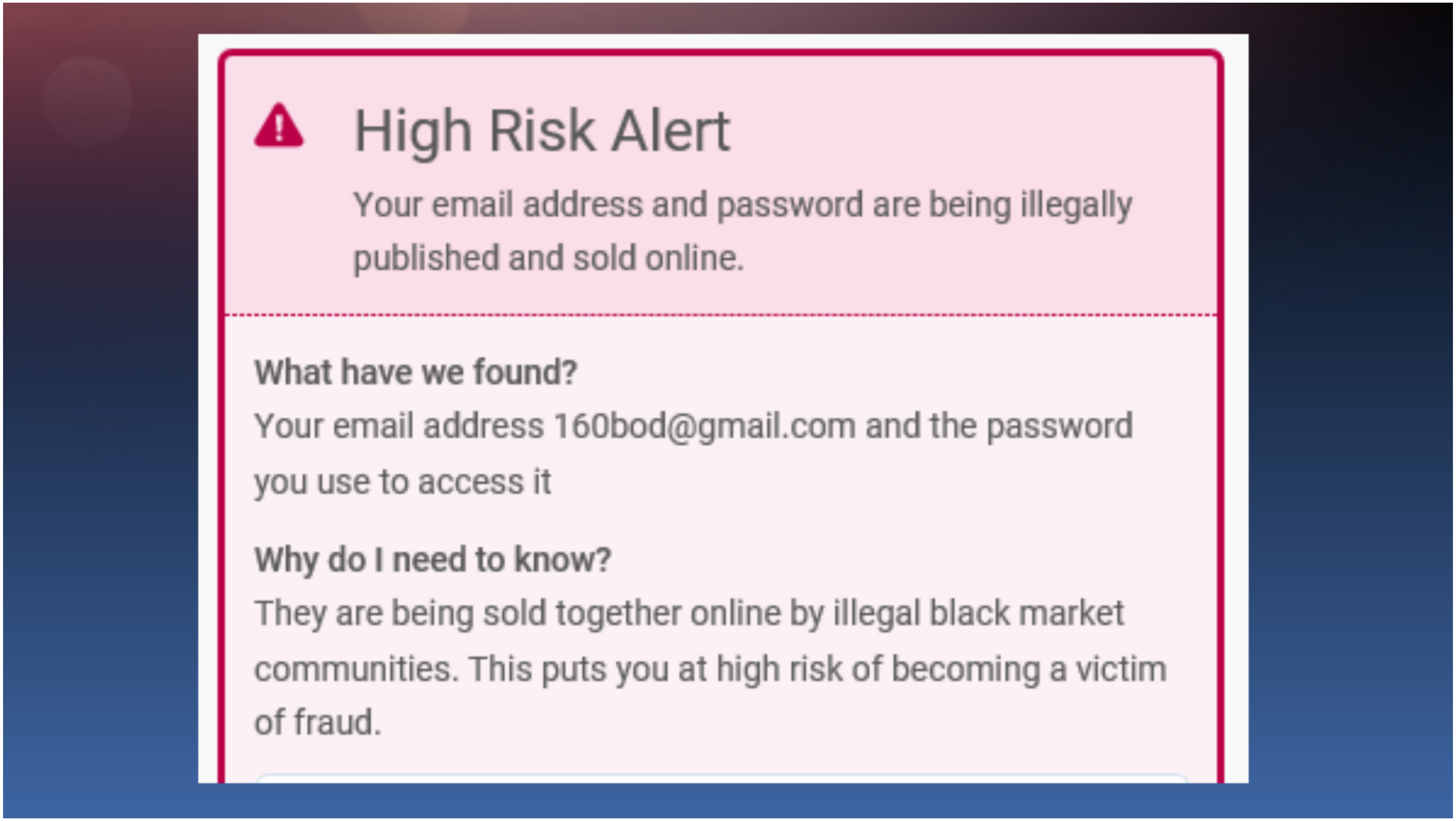
Your email address and password are being illegally published and sold online.

What have we found?

Your email address 160bod@gmail.com and the password you use to access it

Why do I need to know?

They are being sold together online by illegal black market communities. This puts you at high risk of becoming a victim of fraud.



High Risk Alert

Your email address and password are being illegally published and sold online.

What have we found?

Your email address 160bod@gmail.com and the password you use to access it

Why do I need to know?

They are being sold together online by illegal black market communities. This puts you at high risk of becoming a victim of fraud.

CreditExpert

from Experian®

Simple rules for a first line of defence

Simple rules for a first line of defence

Educate your employees about the risks

Simple rules for a first line of defence

Educate your employees about the risks

Install all security updates when released

Simple rules for a first line of defence

Educate your employees about the risks

Install all security updates when released

Consider information you place on the web

Simple rules for a first line of defence

Educate your employees about the risks

Install all security updates when released

Consider information you place on the web

Ensure all internal firewalls are always on

Simple rules for a first line of defence

Educate your employees about the risks

Install all security updates when released

Consider information you place on the web

Ensure all internal firewalls are always on

Introduce clear desk policies

Simple rules for a first line of defence

Educate your employees about the risks

Install all security updates when released

Consider information you place on the web

Ensure all internal firewalls are always on

Introduce clear desk policies

Vet third-party contractors

Simple rules for a first line of defence

Educate your employees about the risks

Install all security updates when released

Consider information you place on the web

Ensure all internal firewalls are always on

Introduce clear desk policies

Vet third-party contractors

Get Cyber Crime Insurance

Simple rules for a first line of defence

Educate your employees about the risks

Install all security updates when released

Consider information you place on the web

Ensure all internal firewalls are always on

Introduce clear desk policies

Vet third-party contractors

Get Cyber Crime Insurance

Lock unattended computers

Simple rules for a first line of defence

Educate your employees about the risks

Install all security updates when released

Consider information you place on the web

Ensure all internal firewalls are always on

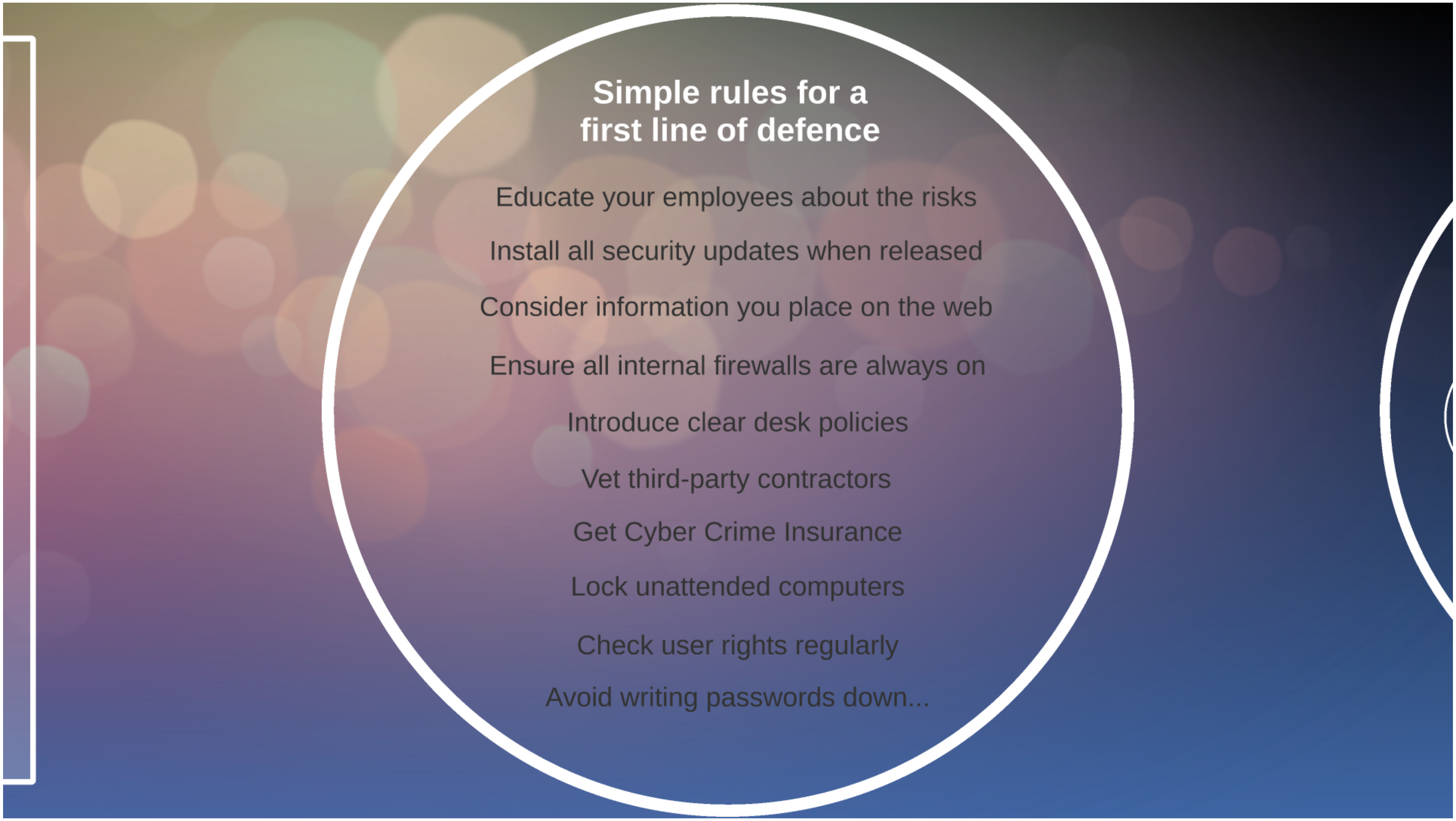
Introduce clear desk policies

Vet third-party contractors

Get Cyber Crime Insurance

Lock unattended computers

Check user rights regularly



Simple rules for a first line of defence

Educate your employees about the risks

Install all security updates when released

Consider information you place on the web

Ensure all internal firewalls are always on

Introduce clear desk policies

Vet third-party contractors

Get Cyber Crime Insurance

Lock unattended computers

Check user rights regularly

Avoid writing passwords down...

Password Policies

Minimum 13 characters

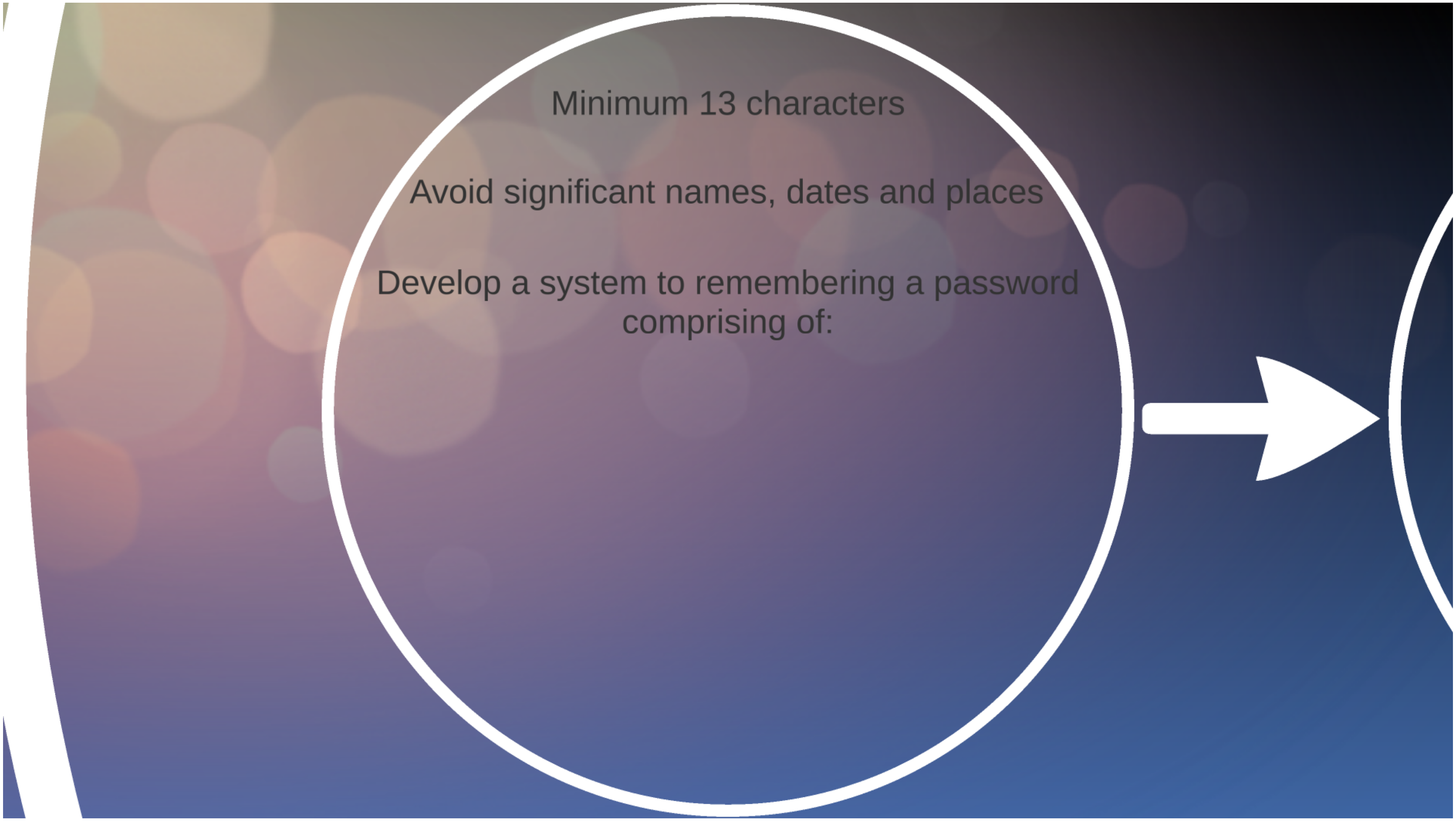
Example Core Password

http://www.amazon.co.uk

Minimum 13 characters

Minimum 13 characters

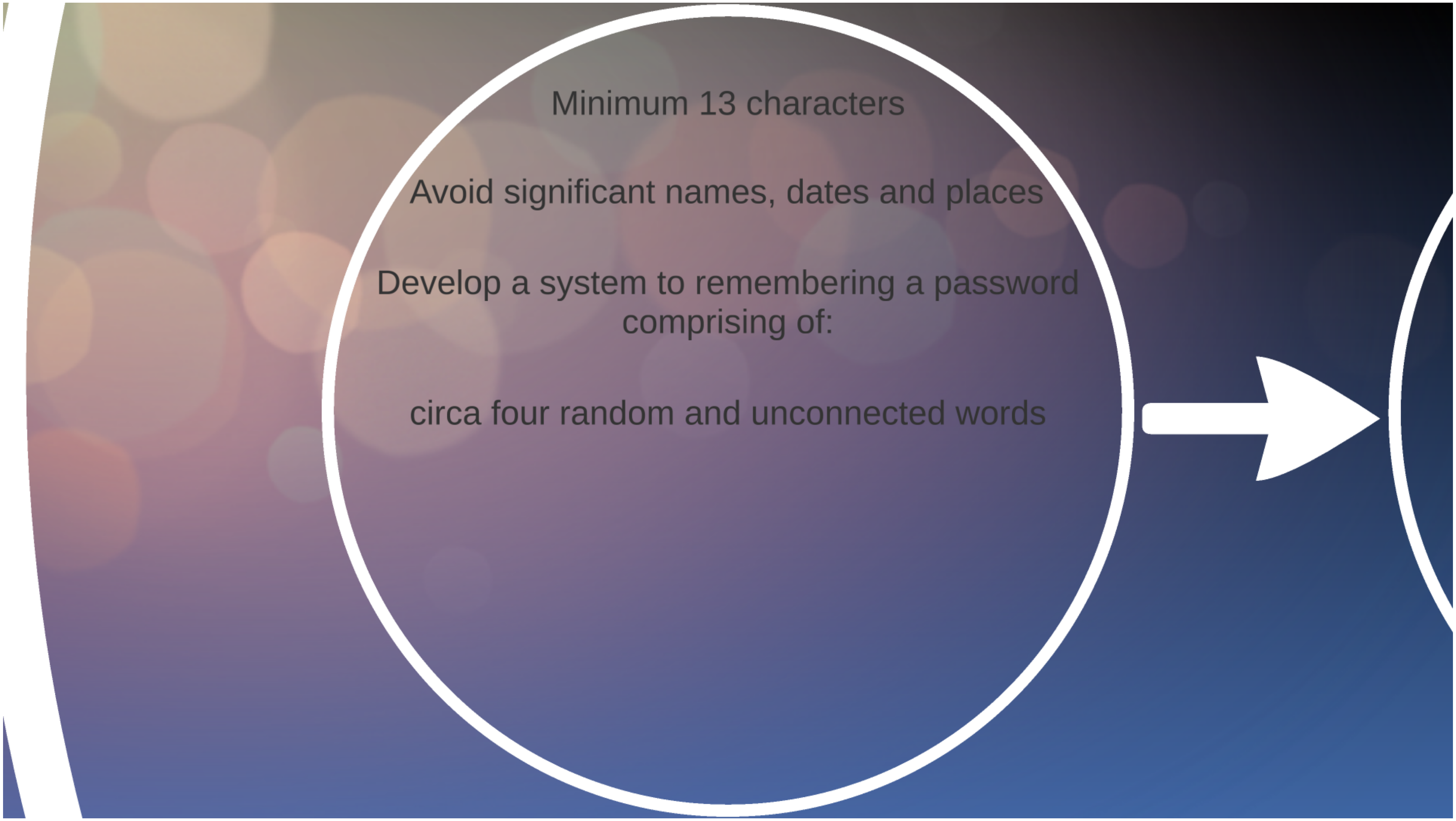
Avoid significant names, dates and places



Minimum 13 characters

Avoid significant names, dates and places

Develop a system to remembering a password comprising of:

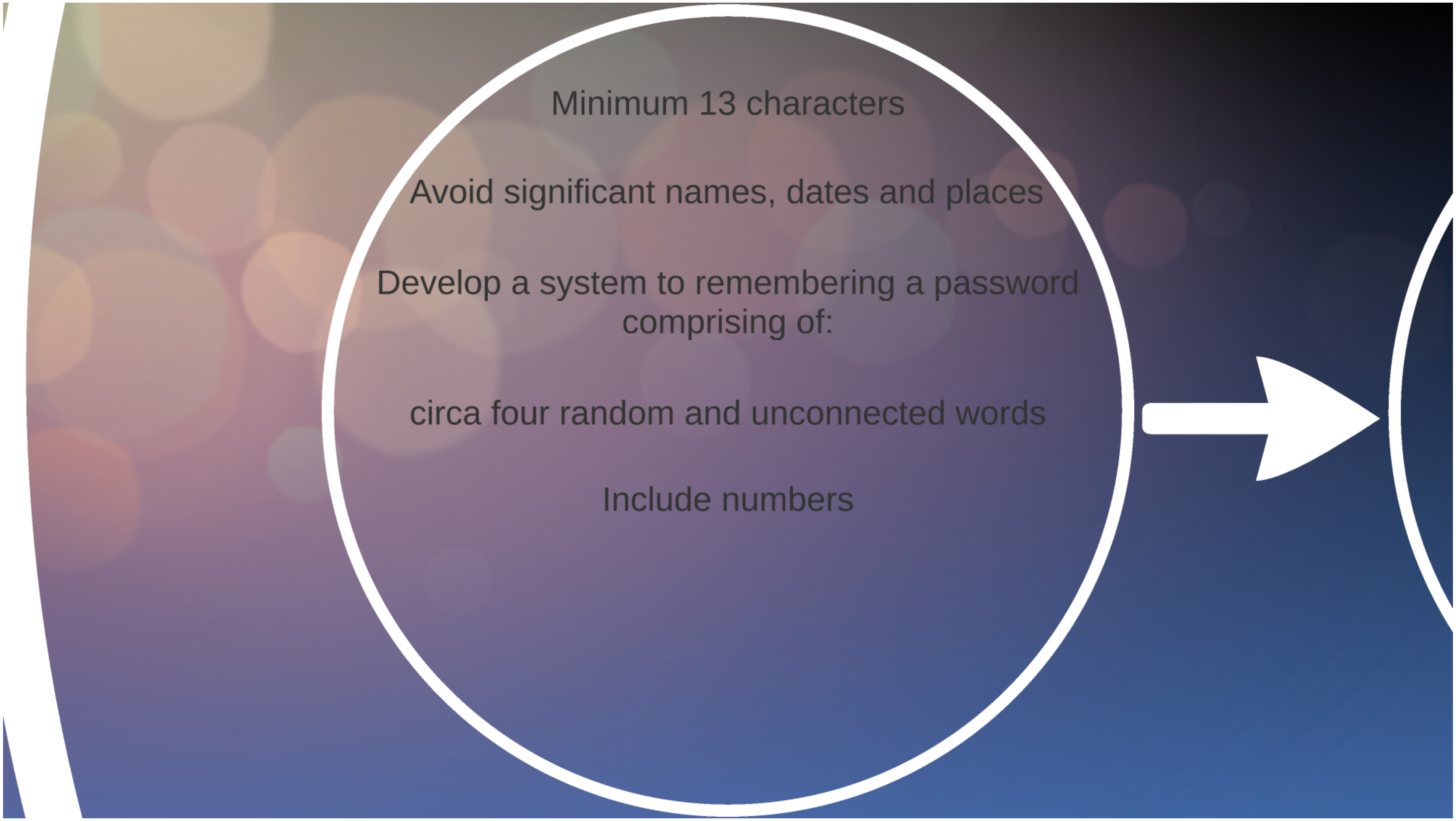


Minimum 13 characters

Avoid significant names, dates and places

Develop a system to remembering a password comprising of:

circa four random and unconnected words



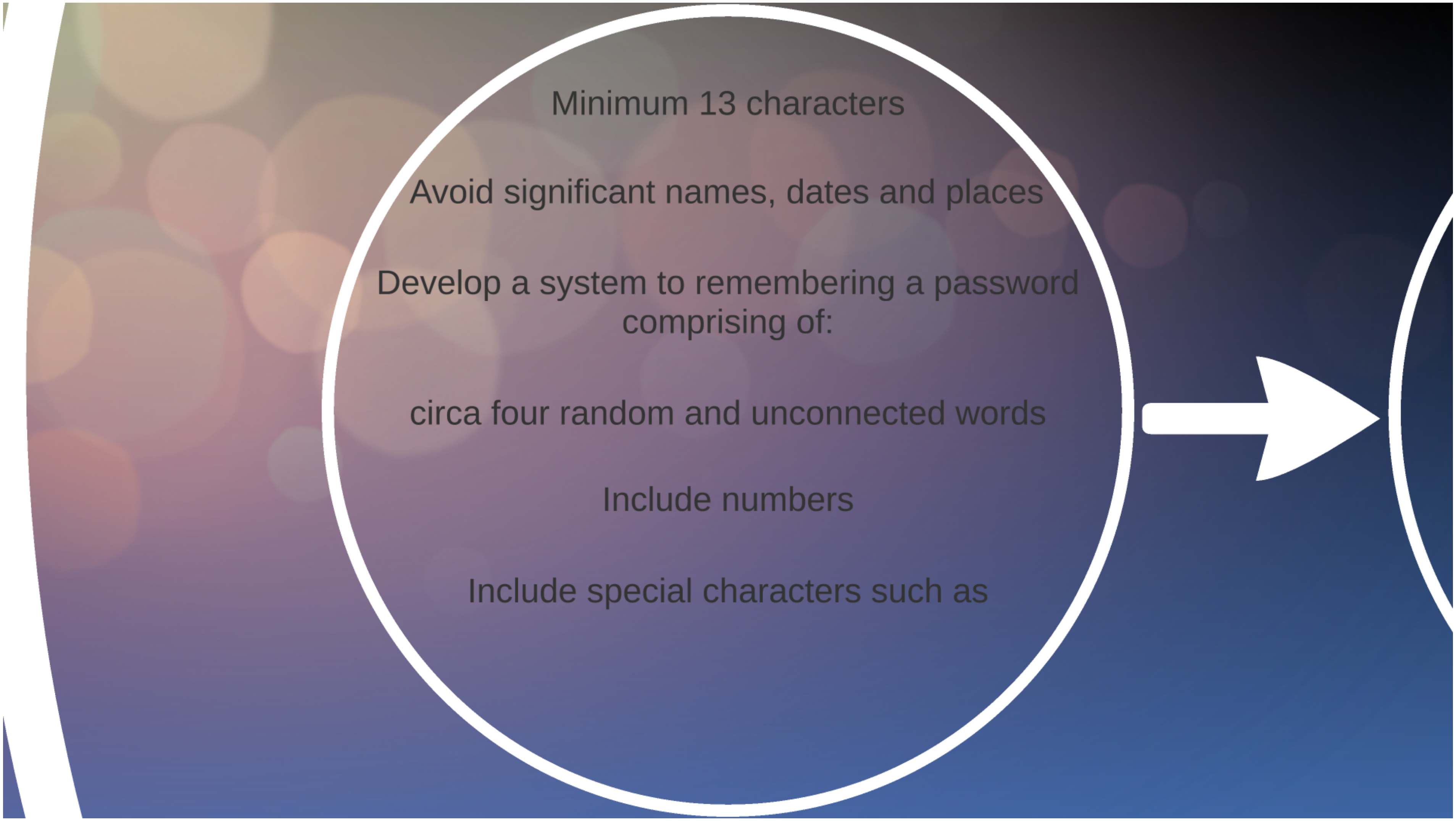
Minimum 13 characters

Avoid significant names, dates and places

Develop a system to remembering a password comprising of:

circa four random and unconnected words

Include numbers



Minimum 13 characters

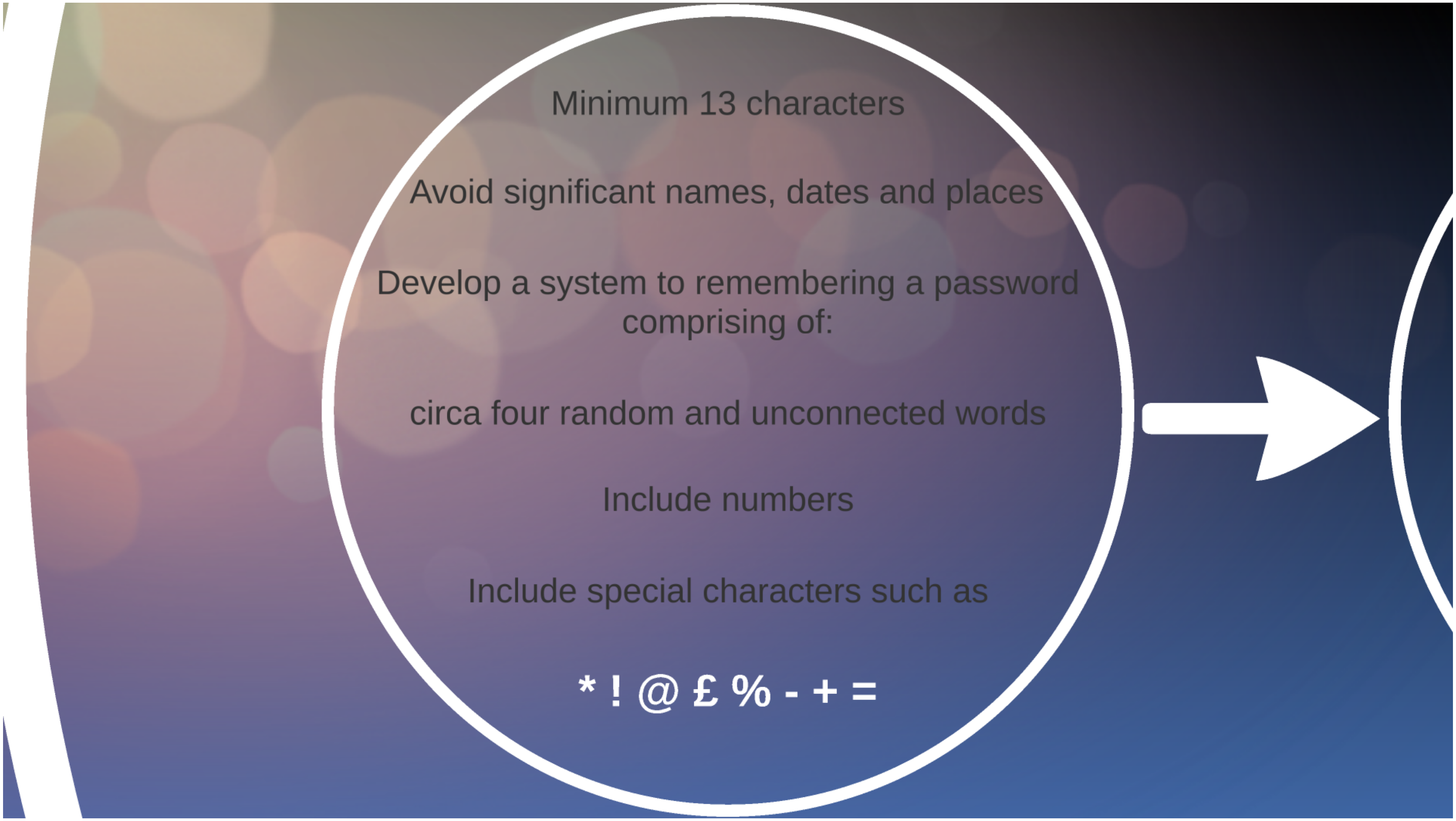
Avoid significant names, dates and places

Develop a system to remembering a password comprising of:

circa four random and unconnected words

Include numbers

Include special characters such as



Minimum 13 characters

Avoid significant names, dates and places

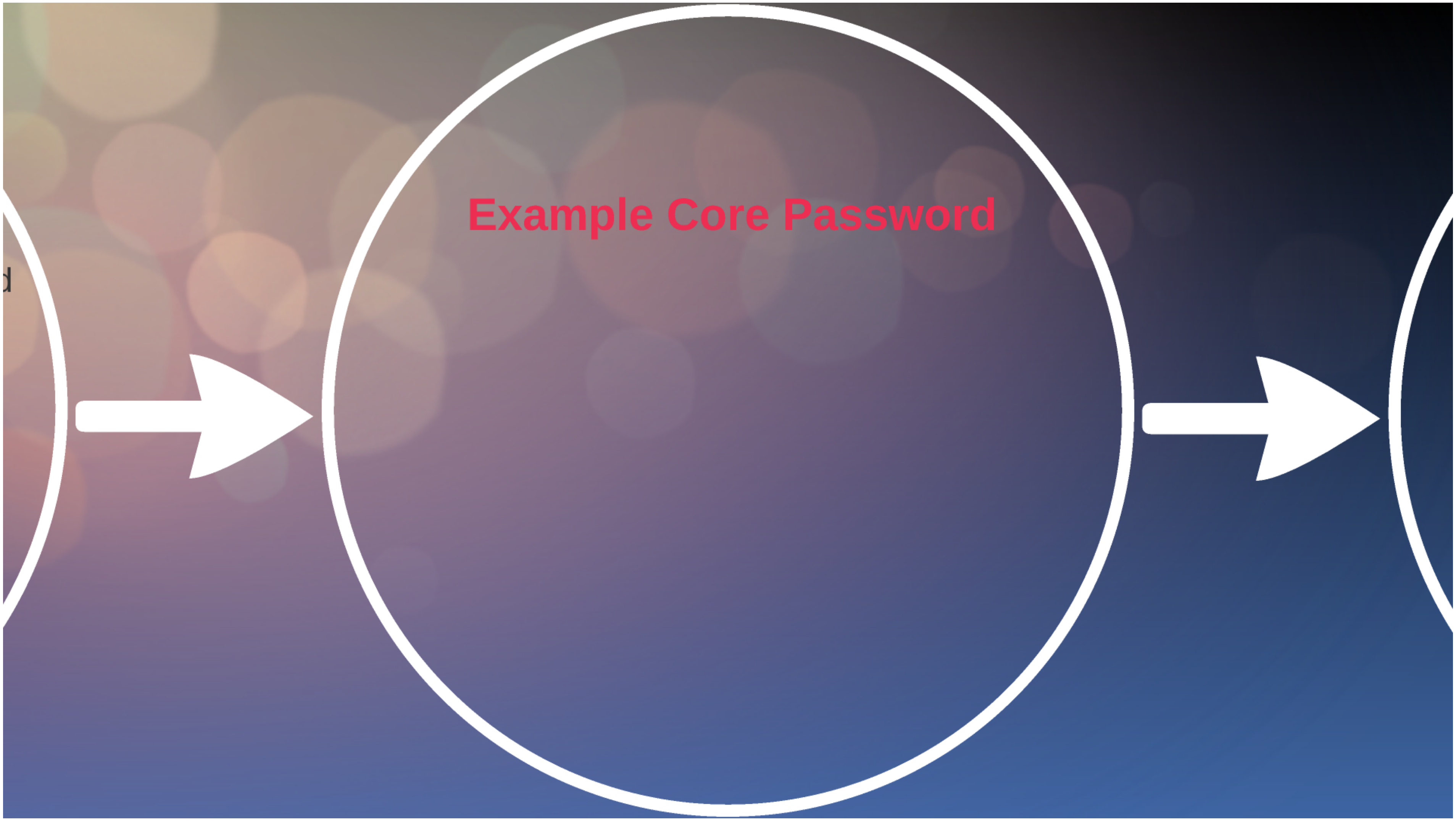
Develop a system to remembering a password comprising of:

circa four random and unconnected words

Include numbers

Include special characters such as

*** ! @ £ % - + =**



d

Example Core Password

Example Core Password

4Pigs2CoffeecupsWanderedBack*!

Example Core Password

4Pigs2CoffeecupsWanderedBack*!

Website specific

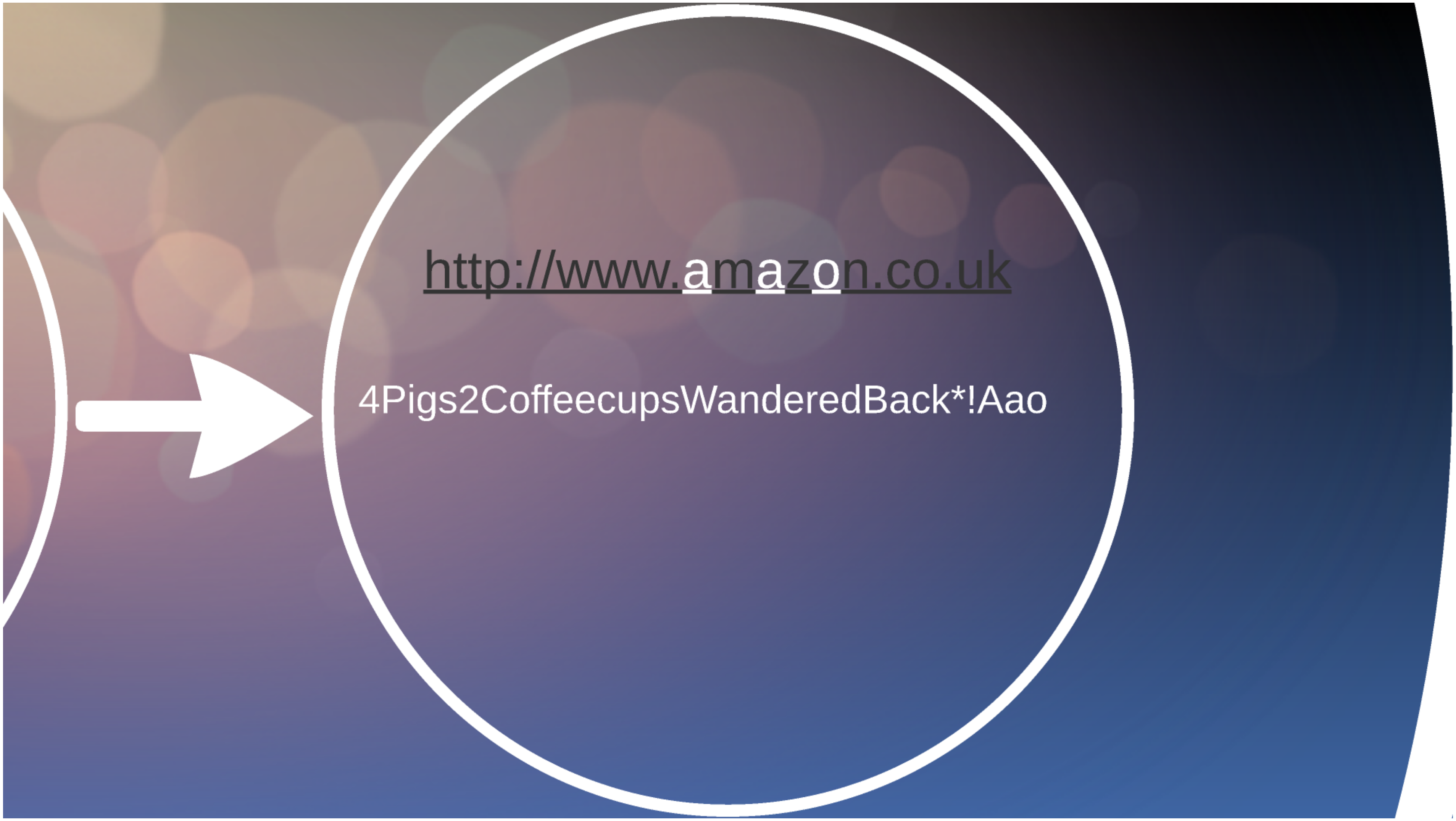
Example Core Password

4Pigs2CoffeecupsWanderedBack*!

Website specific

Core password, plus 1st, 3rd and 5th letters of the website address

http://www.amazon.co.uk



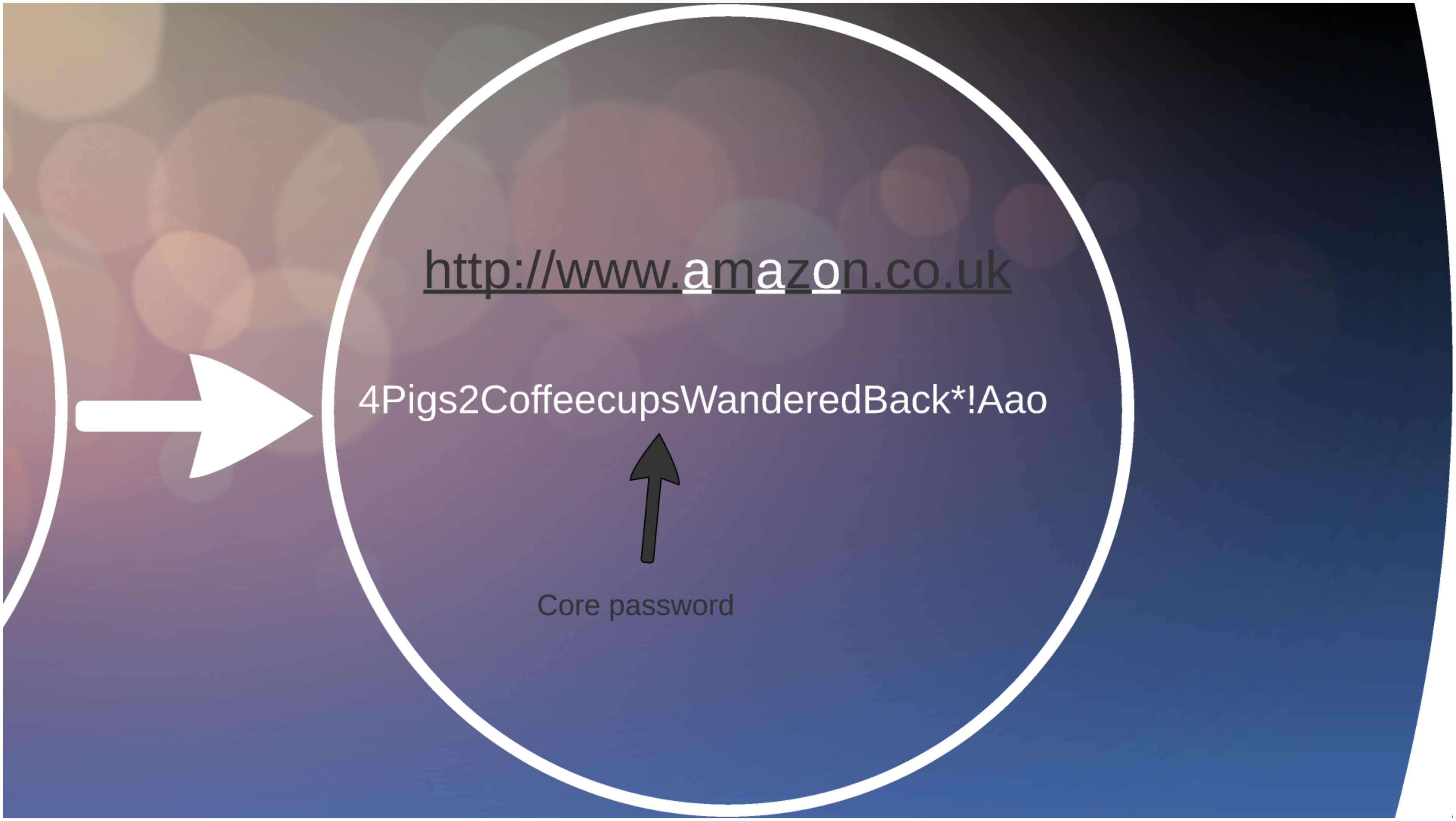
http://www.amazon.co.uk

4Pigs2CoffeecupsWanderedBack*!Aao

http://www.amazon.co.uk

4Pigs2CoffeecupsWanderedBack*!Aao

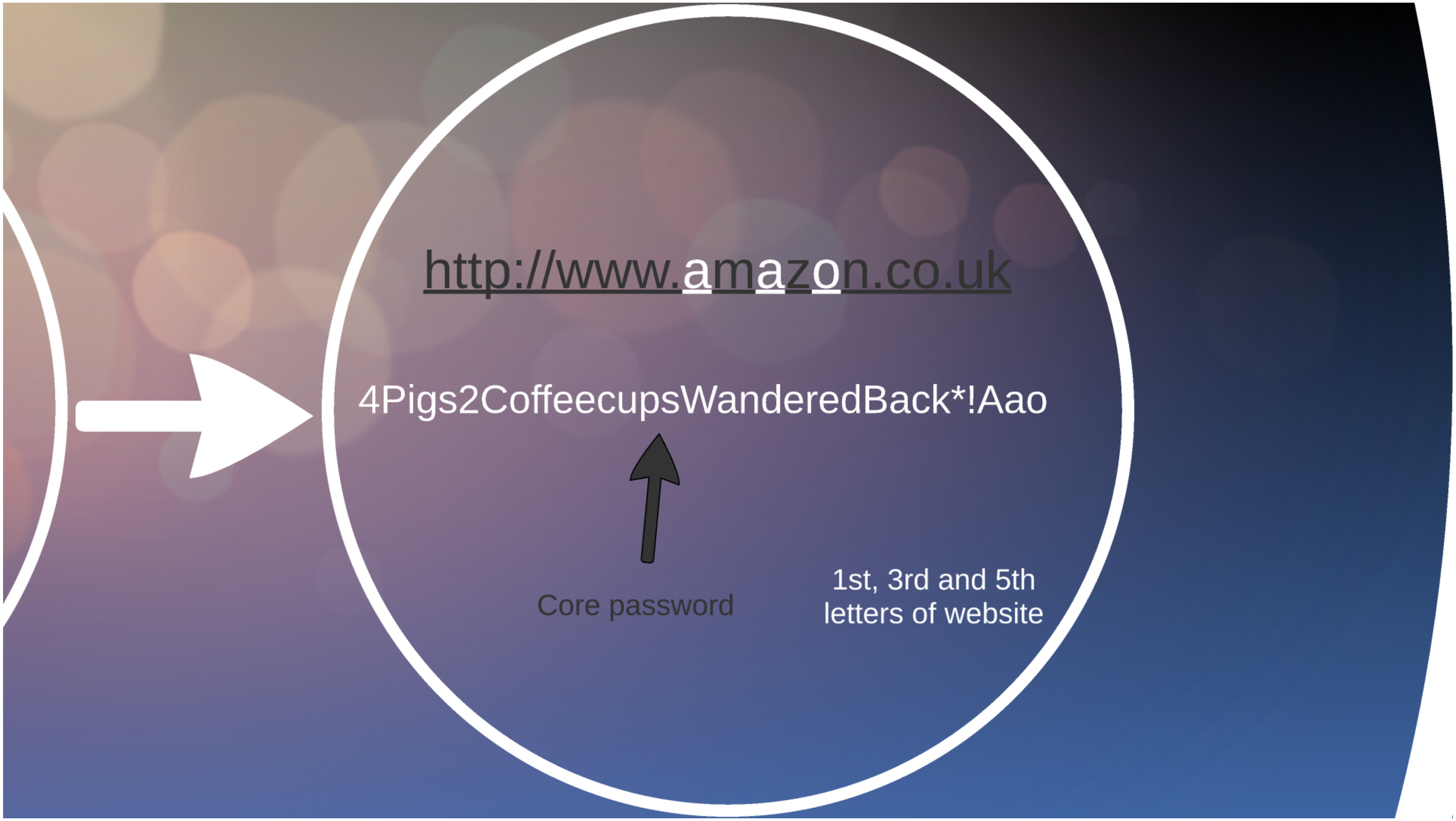
Core password



http://www.amazon.co.uk

4Pigs2CoffeecupsWanderedBack*!Aao

Core password

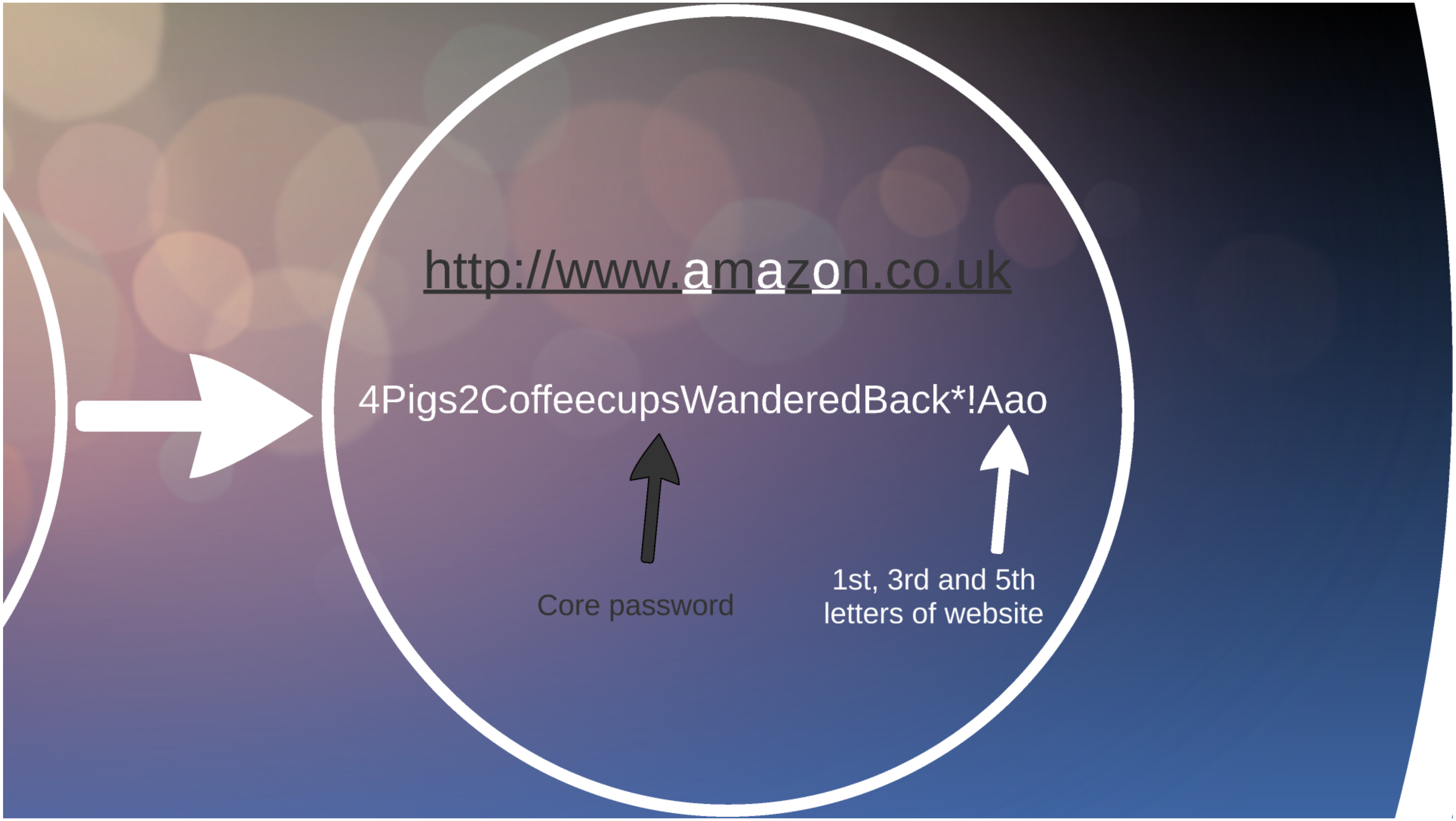


http://www.amazon.co.uk

4Pigs2CoffeecupsWanderedBack*!Aao

Core password

1st, 3rd and 5th
letters of website

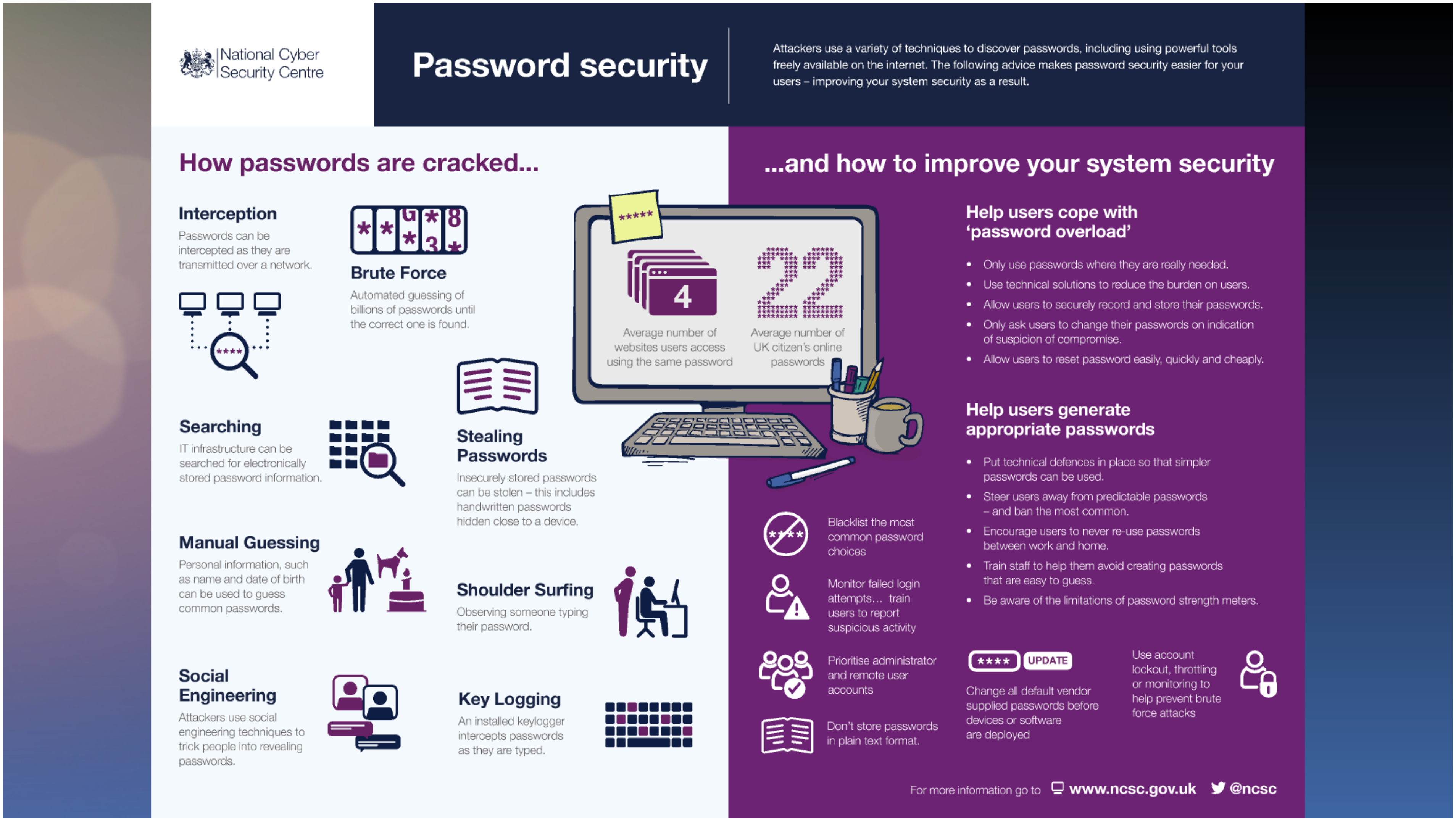


http://www.amazon.co.uk

4Pigs2CoffeecupsWanderedBack*!Aao

Core password

1st, 3rd and 5th
letters of website



National Cyber Security Centre

Password security

Attackers use a variety of techniques to discover passwords, including using powerful tools freely available on the internet. The following advice makes password security easier for your users – improving your system security as a result.

How passwords are cracked...

Interception

Passwords can be intercepted as they are transmitted over a network.

Brute Force

Automated guessing of billions of passwords until the correct one is found.

Searching

IT infrastructure can be searched for electronically stored password information.

Stealing Passwords

Insecurely stored passwords can be stolen – this includes handwritten passwords hidden close to a device.

Manual Guessing

Personal information, such as name and date of birth can be used to guess common passwords.

Shoulder Surfing

Observing someone typing their password.

Social Engineering

Attackers use social engineering techniques to trick people into revealing passwords.

Key Logging

An installed keylogger intercepts passwords as they are typed.

4

Average number of websites users access using the same password

22

Average number of UK citizen's online passwords

...and how to improve your system security

Help users cope with 'password overload'

- Only use passwords where they are really needed.
- Use technical solutions to reduce the burden on users.
- Allow users to securely record and store their passwords.
- Only ask users to change their passwords on indication of suspicion of compromise.
- Allow users to reset password easily, quickly and cheaply.

Help users generate appropriate passwords

- Put technical defences in place so that simpler passwords can be used.
- Steer users away from predictable passwords – and ban the most common.
- Encourage users to never re-use passwords between work and home.
- Train staff to help them avoid creating passwords that are easy to guess.
- Be aware of the limitations of password strength meters.

Blacklist the most common password choices

Monitor failed login attempts… train users to report suspicious activity

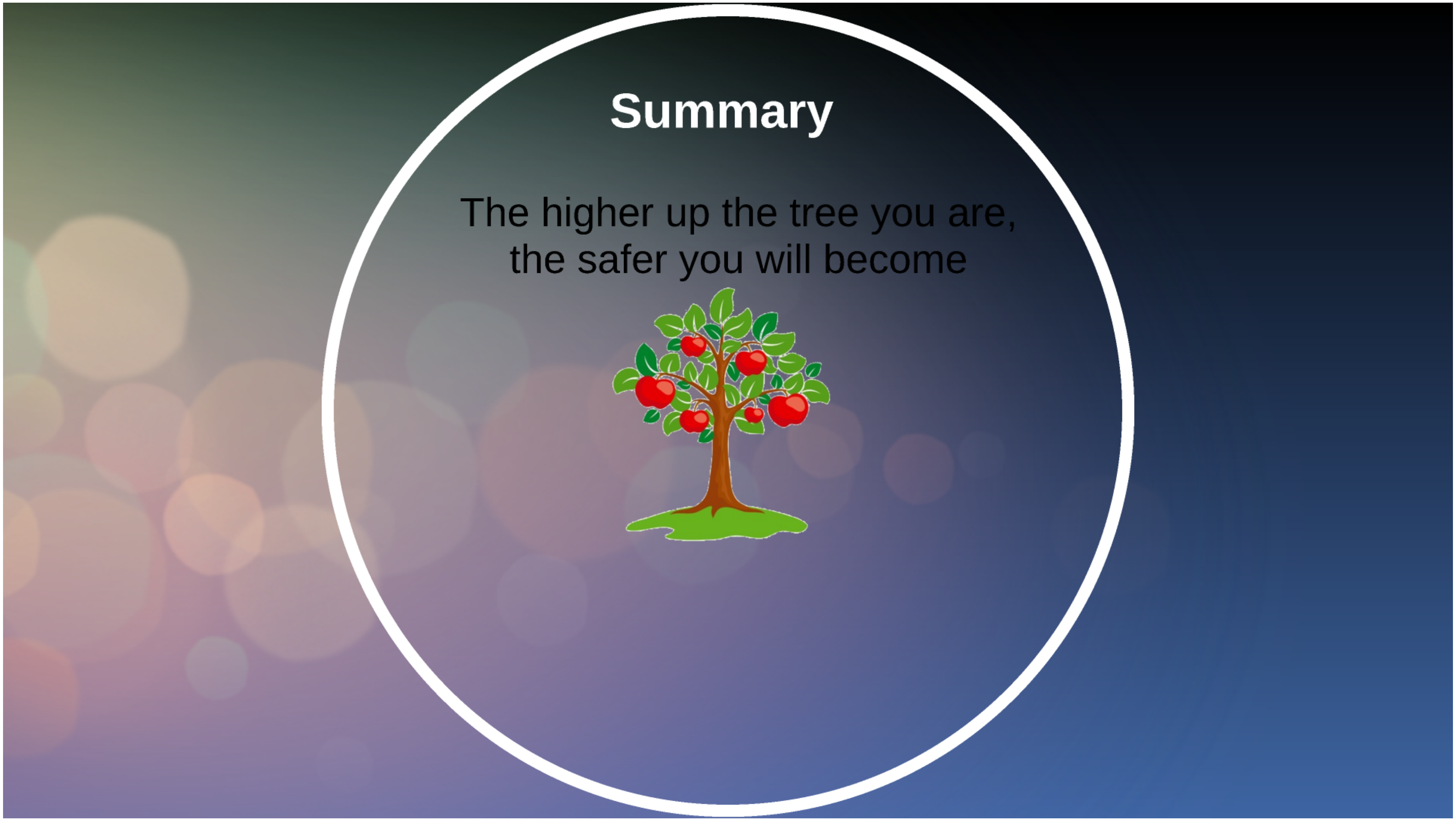
Prioritise administrator and remote user accounts

Don't store passwords in plain text format.

Change all default vendor supplied passwords before devices or software are deployed

Use account lockout, throttling or monitoring to help prevent brute force attacks

For more information go to www.ncsc.gov.uk @ncsc



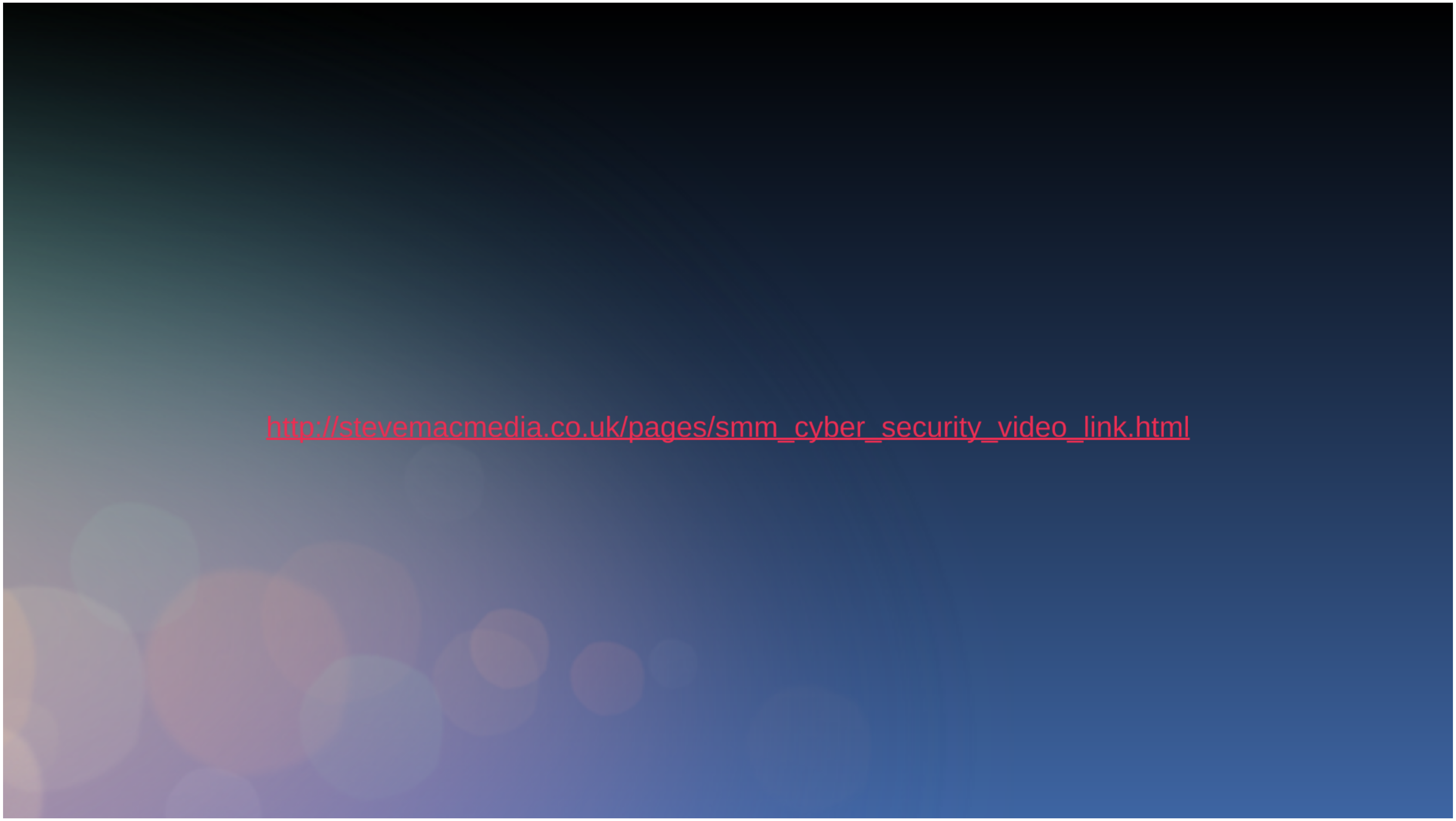
Summary

The higher up the tree you are,
the safer you will become

Summary

The higher up the tree you are,
the safer you will become

To beat a hacker...
you need to think like one!



http://stevemacmedia.co.uk/pages/smm_cyber_security_video_link.html

Any Questions?

SteveMac MEDIA

Steve McLaughlin (Director)

Steve Mac Media Limited
90-92 King Street
Maidstone
Kent ME14 1BH

Mobile: 07919 406224
www.stevemacmedia.co.uk
steve@stevemacmedia.co.uk

CERTIFIED SECURITY TESTING ASSOCIATE
CSTA
ETHICAL HACKING

CERTIFIED FORENSIC INVESTIGATION PRACTITIONER
CFIP
COMPUTER FORENSICS