

Cybersecurity

October 2019





designed by freepik.com

Social Engineering is defined as ...

Noun

1. the use of centralized planning in an attempt to manage social change and regulate the future development and behaviour of a society.
2. (in the context of information security) the use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes.

Source: dictionary.com



“Social engineering is defined as any act that influences a person to take an action that may or may not be in their best interest.”

Chris Hadnagy, *Social Engineering: The Art of Human Hacking.*



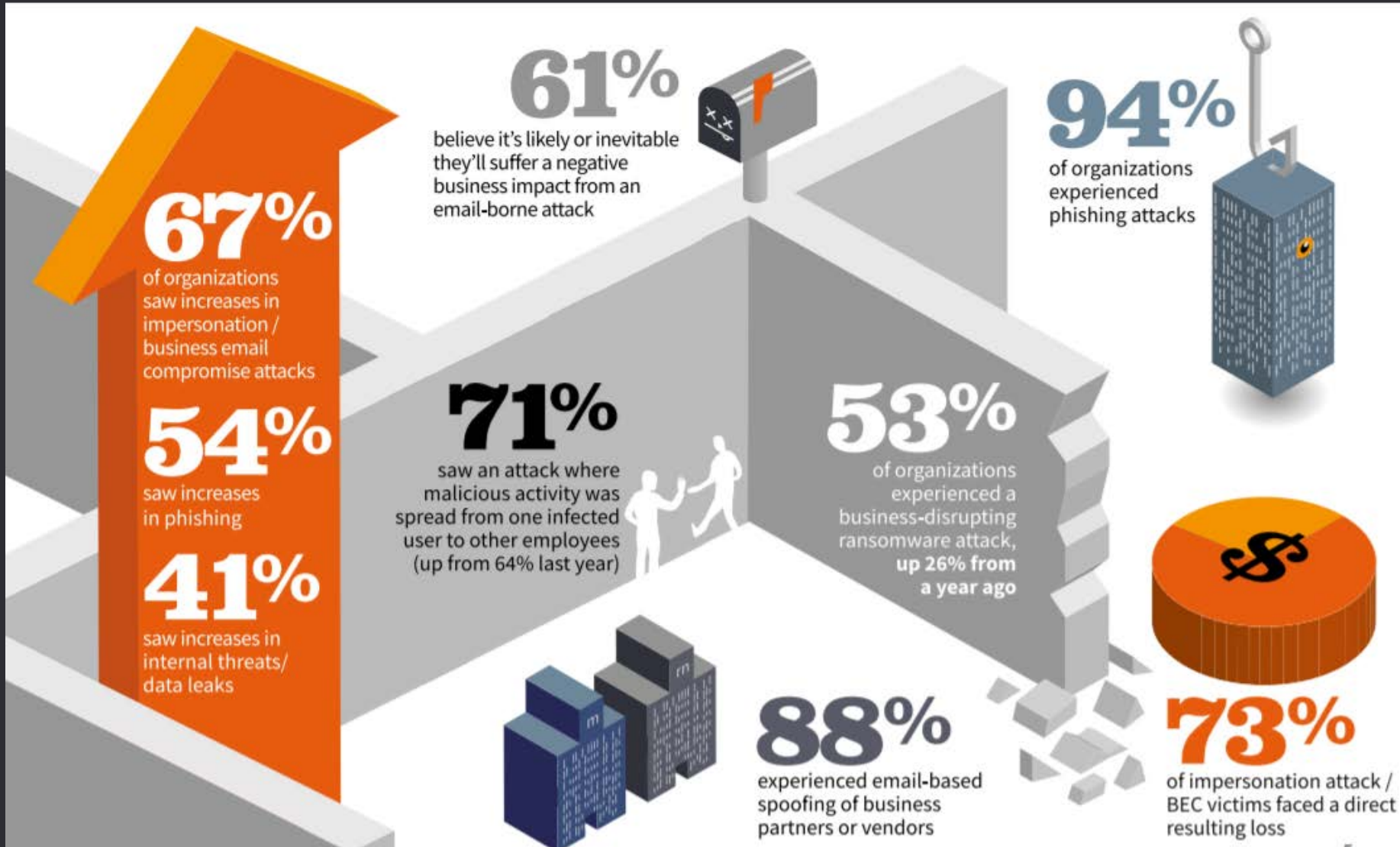
Types of social engineering attacks

- Impersonation
- Phishing
- Spear phishing
- Whaling
- Vishing
- SMiShing
- Baiting
- Pretexting
- Etc....

Source: <https://www.nextiva.com/blog/social-engineering-attacks.html#s3>



Key findings over the previous 12 months

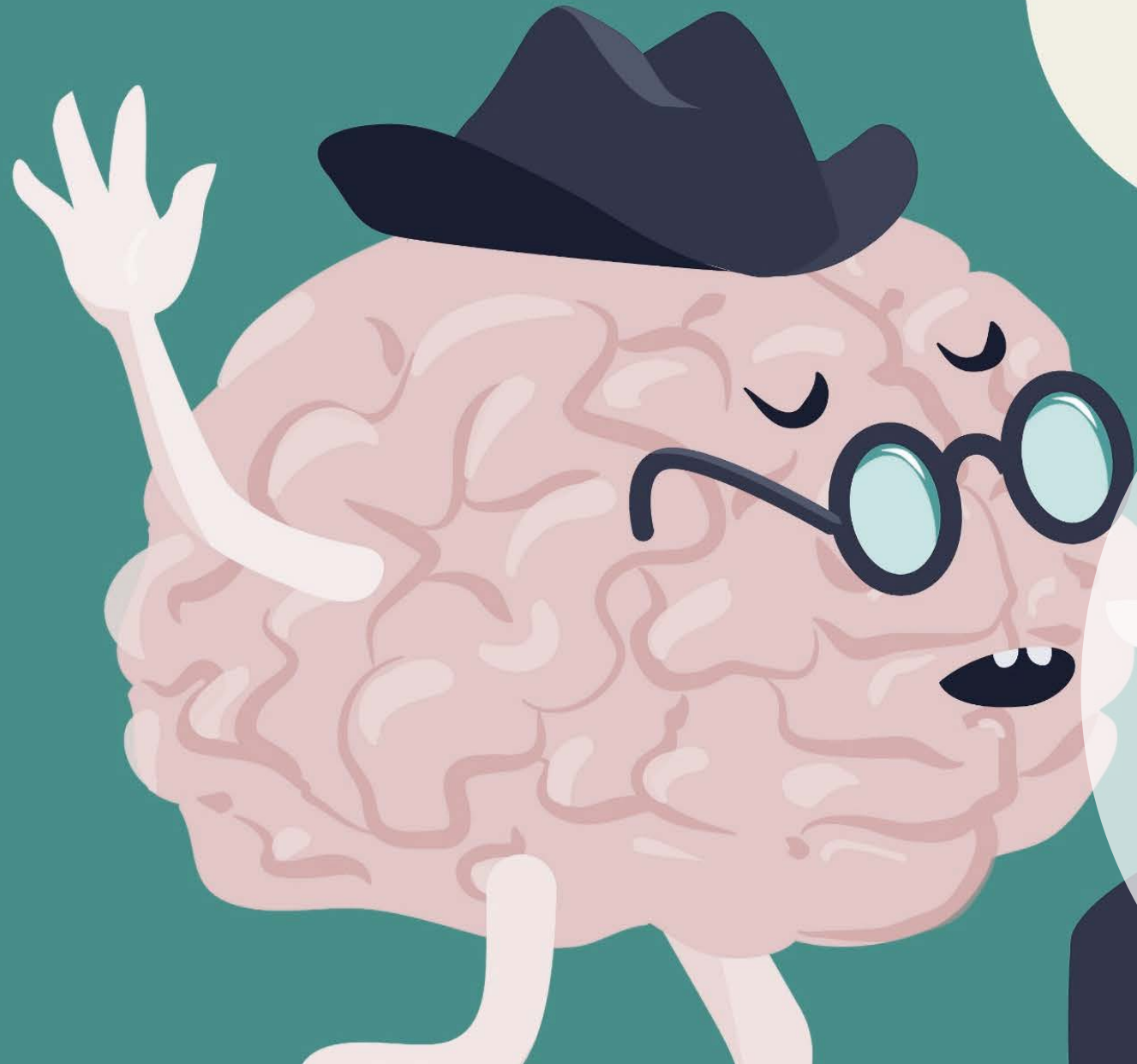




Wallace: Hang on a mo'

2 Awareness Training

What types of cybersecurity and awareness training does your company offer employees?	Total	US	UK	Germany	Netherlands	Australia	South Africa	UAE
Group training sessions with our IT/IT security team	62.3%	64.7%	56.6%	61.3%	52.0%	68.0%	62.0%	72.0%
Interactive videos highlighting best/worst practices to keep in mind	45.0%	56.3%	42.9%	34.7%	35.0%	39.0%	30.0%	61.0%
A formal online test to learn about threats and prompts questions to respond to	44.1%	49.7%	49.7%	32.7%	36.0%	38.0%	31.0%	62.0%
An emailed or printed list of tips to keep in mind	43.7%	42.0%	42.3%	33.3%	29.0%	56.0%	45.0%	68.0%
One-on-one training sessions with our IT/IT security team	43.5%	45.0%	32.6%	47.3%	45.0%	43.0%	35.0%	60.0%
Sends prompts for me to note whether or not a link is "safe" prior to a allowing me to visit certain websites	38.4%	45.3%	31.4%	23.3%	41.0%	36.0%	37.0%	54.0%
Other	0.6%	0.7%	0.6%	0.7%	1.0%	0.0%	1.0%	0.0%
My company doesn't provide any training	2.0%	1.3%	2.9%	1.3%	4.0%	1.0%	4.0%	0.0%
Number of respondents	1025	300	175	150	100	100	100	100



BYE!

“There’s no patch
for human
stupidity!”

Source: The Hacker News - Social Engineering Skype
Support team to hack any account instantly



University of Cape Town
Universiteit van Kaapstad • Umkhonto we Sizwe

AVOID DEATH

Source: Bob Dorigo Jones. (2007). *Remove Child Before Folding: The 101 Stupidest, Silliest, and Wackiest Warning Labels Ever* (1st edition). Grand Central Publishing.



AVOID DEATH

BEFORE REMOVING SEAT BELT AND LEAVING SEAT:

- LOWER LIFT ARMS TO GROUND OR REST LIFT ARMS ON STEPS
- STOP ENGINE
- LOCK PARK BRAKE & REMOVE KEYS

UTM



Universiteit van Kaapstad • University of Cape Town • iYunivesithi yaseKapa

*“ We arrive at the
truth, not by the
reason only, but
also by the heart.”*

—Blaise Pascal



Dr. Robert Cialdini | INFLUENCE AT WORK

Source:

<https://www.influenceatwork.com/principles-of-persuasion/>



Principles of **Persuasion**:



Reciprocity



Scarcity



Authority



Consistency



Liking



Consensus



Real-World
Application of the
Principles of
Persuasion

The Experiment



Student Networking

ADMISSIONS

RESEARCH

OFF-CAMPUS

Rhodes > Student Networking > Off-campus

Off-campus Internet access

Rhodes University provides Internet access in a number of private flat complexes and student housing in town, in conjunction with partner service providers. If you live in one of these locations, you can sign up for access. Please note that, unlike [eduroam](#), this is a charged-for service.

At present, wired network access is available in all complexes, while Wi-Fi access is in the early stages of deployment. Wi-Fi access is available in certain complexes, but will be made available in more complexes.

Where is this available?

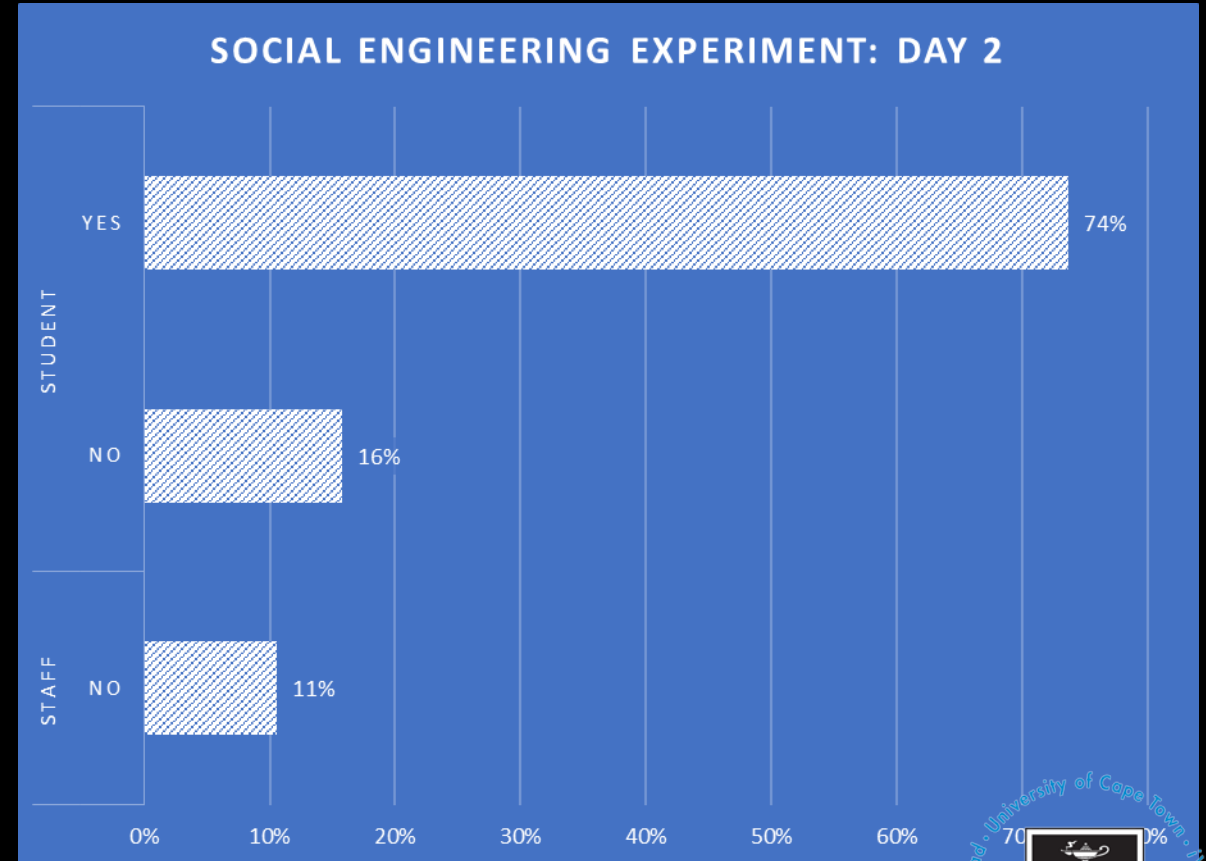
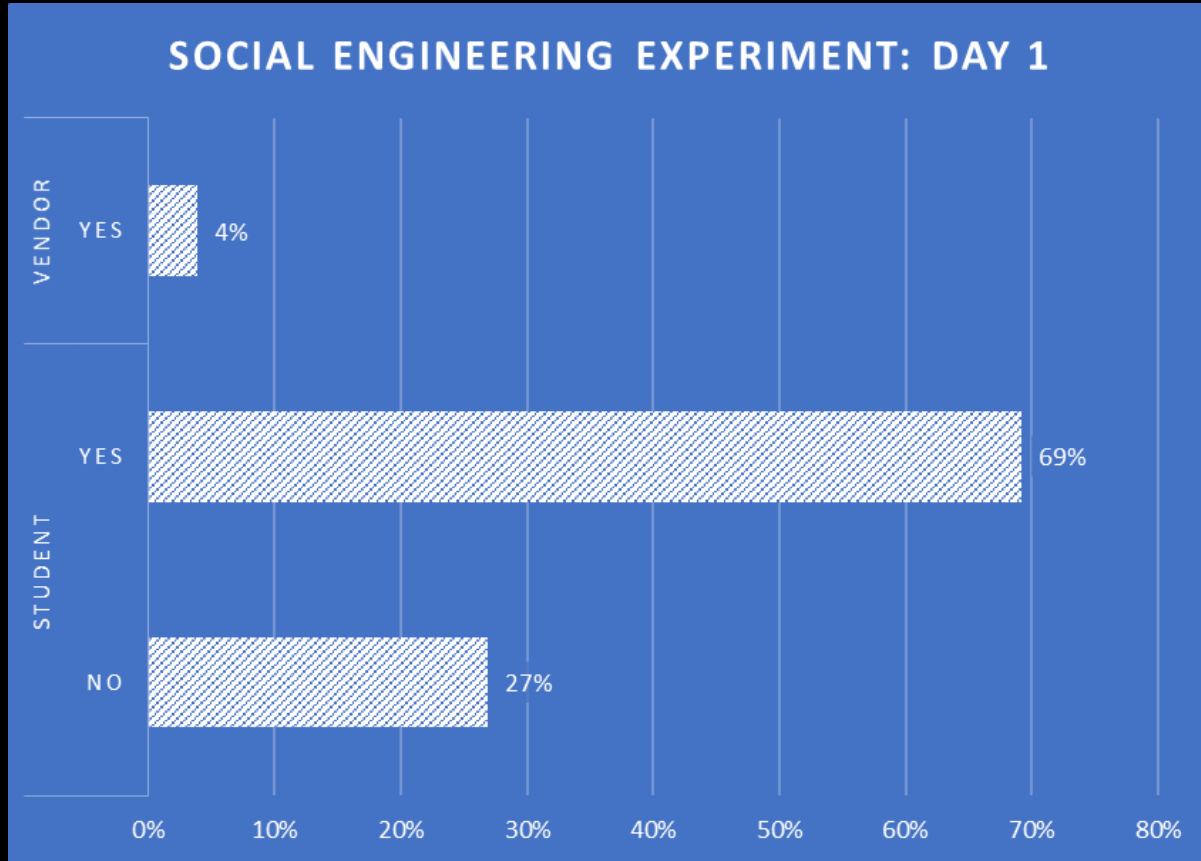
Location	Address	Services	Connected	Surcharge?	Port Faults
		Wi-Fi and wired	2012 / Fibre	Yes	GEEnet

Source: <https://www.ru.ac.za/studentnetworking/offcampus/>

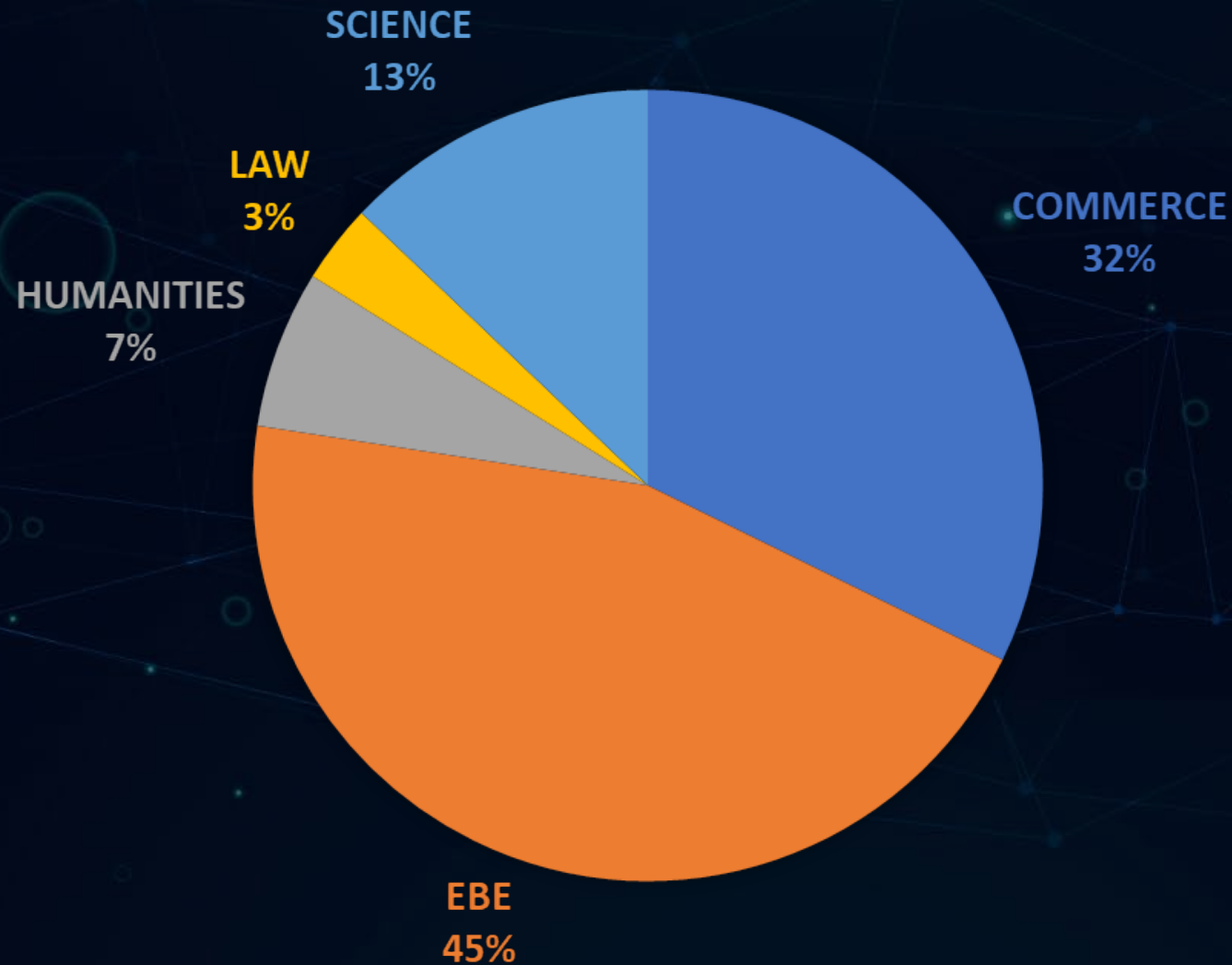
Concept



The Results



Results per Faculty




A Phishing example

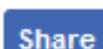
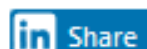


12

Sep

SCAM OF THE WEEK: "The Boss Needs iTunes Gift Cards For Customers... NOW"

 Stu Sjouwerman



If you ever wondered if those iTunes gift card phishes really work, see the below email exchange.

Yep, that overzealous employee actually drove around town from store to store picking up iTunes gift cards for the bad guys because there was a limit on the number of cards that could be bought at any one store at one time.

All told poor Emily bought TWENTY \$100.00 iTunes gift cards for these criminals. Still worse, she put them ON HER OWN PERSONAL CREDIT CARD!



From: John Carpenter <officeexec.mails@inbox.lv>

Sent: Thursday, September 6, 2018 11:20 AM

To: Emily Walker <ewalker@distracted.com>

Subject: Respond

Let me know when you are available. There is something I need you to do.
I am going into a meeting now with limited phone calls, so just reply my email.

John Carpenter

Sent from my iPad

Subject: RE: Respond

Date: 6 September 2018 at 21:24:35

From: Emily Walker <ewalker@distracted.com>

To: John Carpenter <officeexec.mails@inbox.lv>

Did you intend to send this to me?

Emily Walker

Project Manager

Sent from my iPhone

From: John Carpenter <officeexec.mails@inbox.lv>

Sent: Thursday, September 6, 2018 11:28 AM

To: Emily Walker <ewalker@distracted.com>

Subject: RE: Respond

Yes Emily, can you get this done ASAP? I need some couple of gift cards.
There are some listed clients we are presenting the gift cards. How
quickly can you arrange these gift cards because i need to send them
out in less than an hour. I would provide you with the type of gift
cards and amount of each.

Sent from my iPad

Why?



UCT today



The Centre for Higher Education Development partners with the six faculties to ensure students don't just gain access to UCT, but also succeed here. They work to improve UCT's teaching and learning environment.



+/- 6 370

students lived in UCT's 32 catered or self-catering student residences in 2018, while 22 230 students lived off campus.

8 062 undergraduates
- nearly 50% - received financial support in 2018.

Massive open online courses (MOOCs)

15 MOOCs are currently running at UCT, and have attracted more than 230 000 people from over 100 different countries across the globe.

25 km²

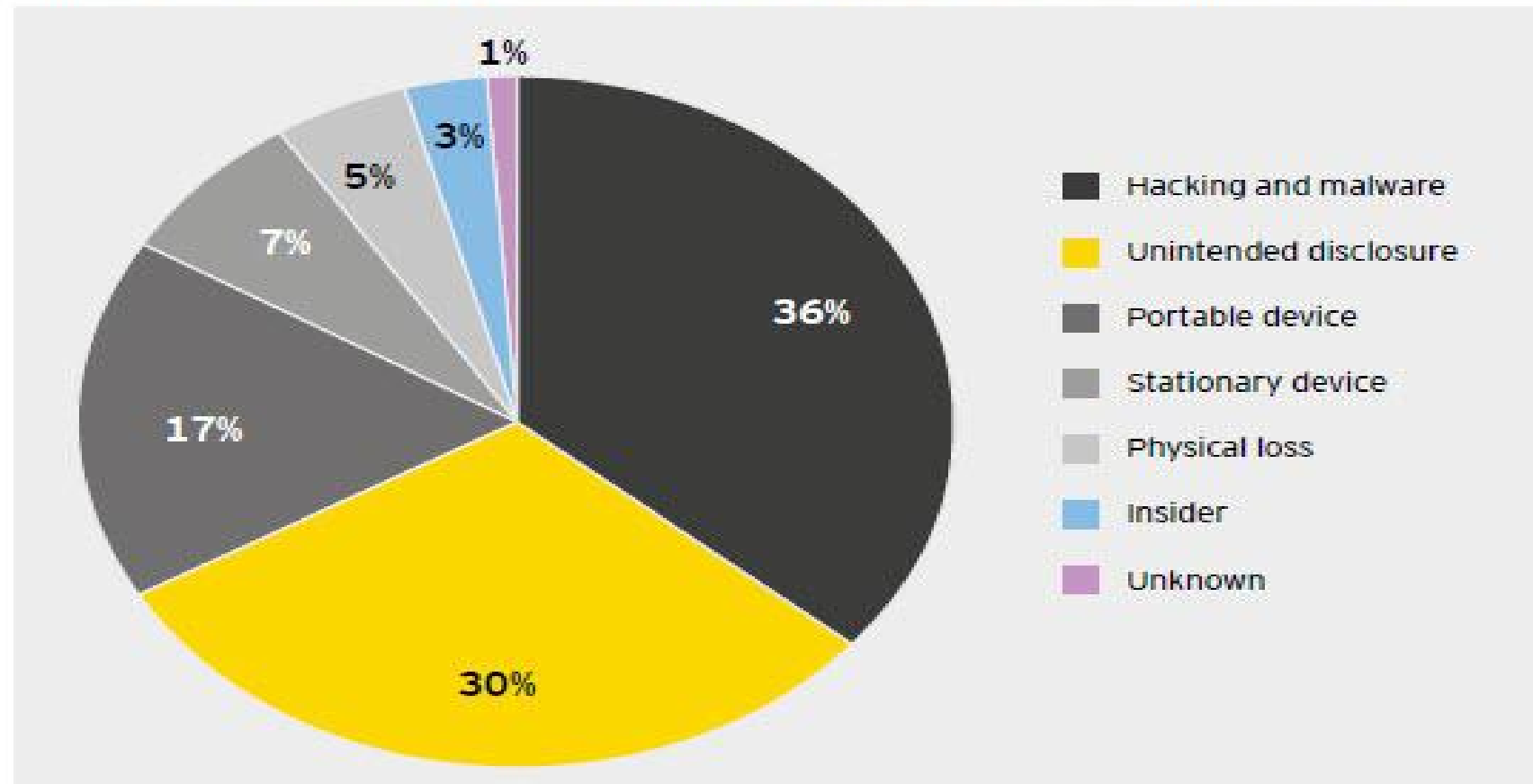
is the total area of UCT's campuses, including upper, middle and lower campus in Rosebank; the health sciences campus in Observatory; the Hiddingh Campus in Gardens; the Graduate School of Business (GSB) Breakwater Campus on the Atlantic Seaboard and the GSB Solution Space in Philippi.

28 600 students and 4 544 staff

In 2018 UCT was home to 28 600 students (17 552 undergraduates, 11 048 postgraduates) and 4 544 staff (1 208 academic and 3 336 professional, administrative support and service staff). Over the course of the year, anywhere between 100 and 1 000 students are employed by the university.

Impact on HEI's

Figure 1. Types of data breaches impacting higher education institutions



<https://consulting.ey.com>



"There are only two types of companies: those that have been hacked and those that will be hacked"

Robert Mueller, Former FBI Director

YOUR CITY HAS BEEN HACKED

Hello Joburg city! Here are Shadow Kill Hackers speaking. All of your servers and data have been hacked. We have dozens of backdoors inside your city.

We have control of everything in your city. We can shut off everything with a button. We also compromised all passwords and sensitive data, such as finance and personal population information.

Your city must pay us 4.0 Bitcoins (thats a very small amount of money) to the following address (19GUXmfkus3YCVNWcoHwgbJSqLusUNZakt) until October 28 17:00PM your time.

If you don't pay on time, we will upload the whole data available to anyone in the internet.

If you pay on time, we will destroy all the data we have, and we will send your IT a full report about how we hacked your systems and your security holes.

Contact us for more information at shadowkill@tutanota.com

Have a nice weekend. Shadow Kill Hackers Group.

OK

Real world examples

EXCLUSIVE: T... vulnerable af... hacked

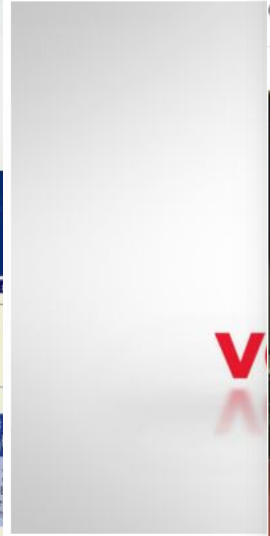
Tuesday 21 May 2013 - 3:05pm



Picture of www.saps.gov.za which w

My Vodaco... exposes su

Rudolph Muller 30 Decem

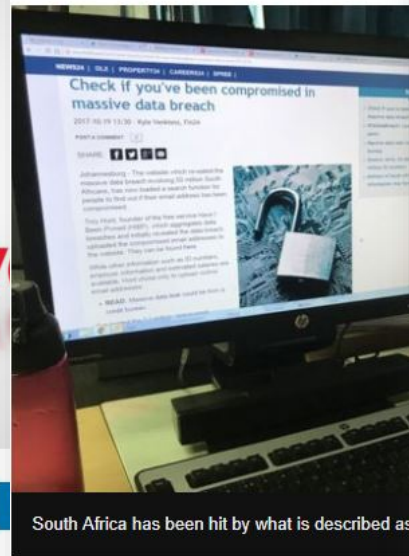


A security flaw in the "M... subscribers' personal de... service providers, avera... details.

Millions caught in s... data breach'

By Pumza Fihlani
BBC News, Johannesburg

© 20 October 2017



South Africa has been hit by what is described as

Authorities in South Africa are investiga... the personal details of more than 30 mil... placing them at risk of identity theft.

Liberty hack the 'biggest breach yet'

Liberty Life is the latest SA firm to have its breached and has potentially exposed the personal details of millions

21 JUNE 2018 - 05:00 by TOBY SHAPSHAK



David Munro: Liberty decided not to accede to hackers' demands Freddy Mavunda



NATIONAL

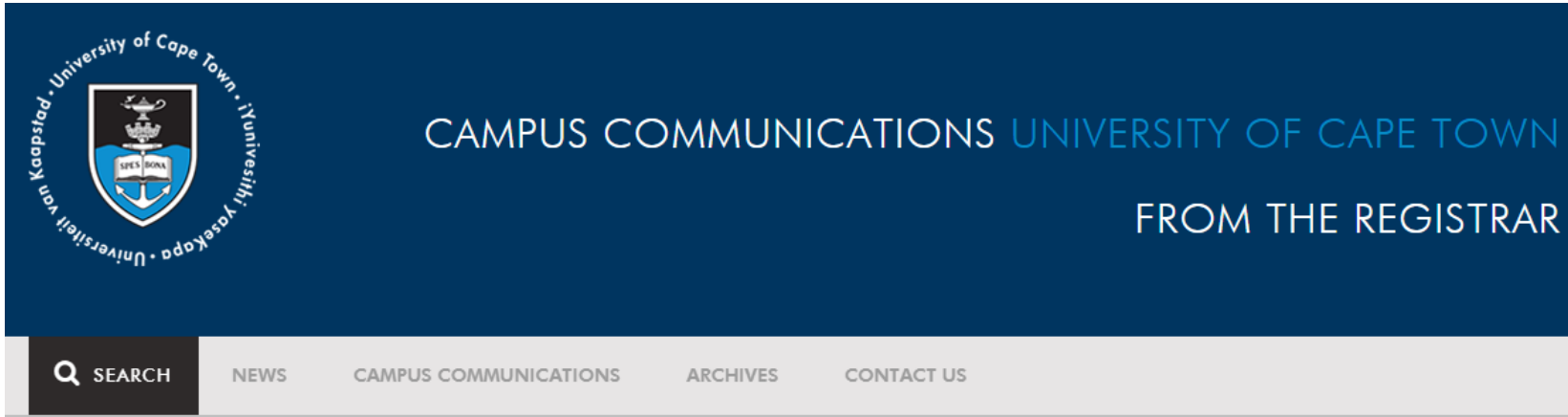
City of Joburg, banks under cyber attack

A group called the Shadow Kill Hackers demands payment of 4.0 bitcoins by October 28 or will upload all hijacked data onto the internet

25 OCTOBER 2019 - 00:25 by CAROL PATON



A UCT example



Addressing irregular access to NBT information

31 MARCH 2019 | ROYSTON PILLAY, REGISTRAR

Dear colleagues and students

The University of Cape Town's (UCT) Centre for Educational Testing for Access and Placement (CETAP) was informed in late January 2019 that certain personal identifiable information (PII) of individuals who wrote their National Benchmark Tests (NBT) had been found online. The NBT system is hosted on a UCT platform.

UCT's **Computer Security Incident Response Team (CSIRT)** conducted a technical assessment of all the system components. This consisted of checking the software comprising the operating system and website applications for potential weaknesses which could have contributed to the exposure of NBT applicant PII.

Most read

→ **DHET publication count: research excellence is more than a numbers game**
17:35, 6 May 2019

↳ **UCT Staff inclusivity survey**



Protecting Your Research Data



Data Classification



Data Encryption

- Encryption may be used to further protect confidential and sensitive research data
- If data is encrypted, ensure that encryption is enabled for encryption in transit and at rest





COMPLIANCE



Legal Considerations

POPI compliance

ECT Act

PAIA

GDPR





Cybercrimes Bill – Regulation of cybercrimes in South Africa

POPI

Record retention constraints

Data subject rights

Security safeguards

Notification of security
compromise

Global guide to data protection

Linklaters About Us Client Services Sectors Find People Locations Insights Careers

Insights // Data Protected

Data Protected Home: Your global guide to data protection

Welcome to Data Protected.

The priority over the last year for most businesses operating in the European Union has been the arrival of the General Data Protection Regulation. This marks the most significant change to privacy regulation in the European Union for over 20 years.

To assist with this process, we have fully updated our guide to the General Data Protection Regulation which is available [here](#). In addition, this edition of Data Protected tracks the national laws adopted to help implement the General Data Protection Regulation. Most jurisdictions have now adopted these laws, though some are still in the processing of finalising their implementing laws. The position is summarised in this [table](#).

The General Data Protection Regulation has been designed with new technology, such as artificial intelligence, in mind. Additional controls on use of automated decision making and mandatory impact assessments should help ensure the safe and ethical use of this technology. We have prepared a detailed report on the use of artificial intelligence, including the interaction with data protection laws, which is available [here](#).

We hope that this report is useful. If you have suggestions about the report, or any other comments, please let us know.

Data Protected - Glossary

Choose a jurisdiction

- Argentina
- Australia
- Austria
- Belgium
- Brazil
- Bulgaria
- Canada
- Croatia
- Cyprus
- Czech Republic
- Denmark
- DIFC



UNIVERSITY OF CAPE TOWN



COMPUTER SECURITY
INCIDENT
RESPONSE TEAM

Mandate



Manage computer security incidents



Investigation and assessment



Ensure return to normal operating conditions



Perform digital forensics



Inform the UCT senior leadership



Manage potential risks



Prevent the recurrence of incidents



Provide education and advice



Announce potential vulnerabilities and threats



Represent UCT at a national and international level



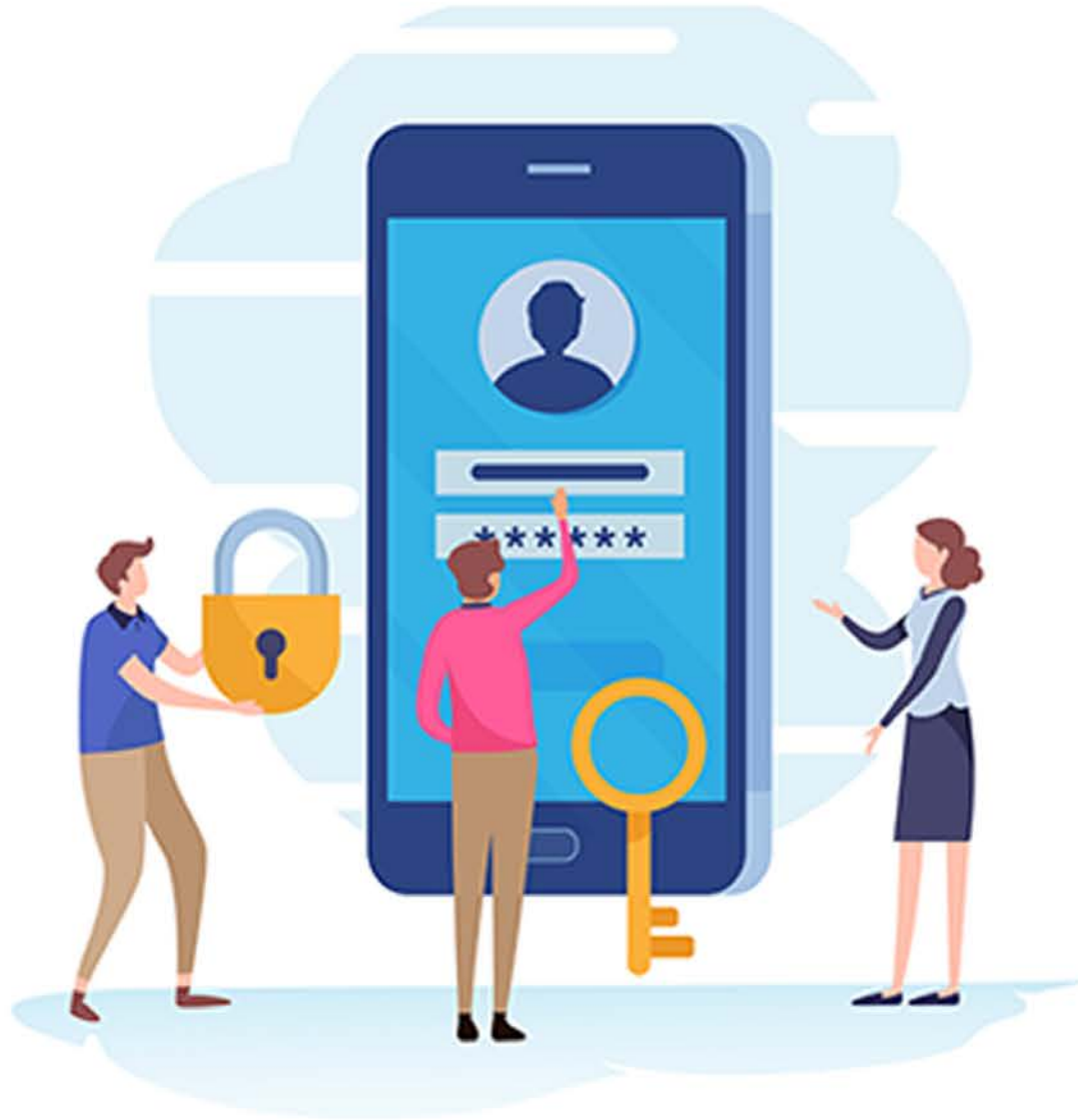


csirt@uct.ac.za



csirt.uct.ac.za

CYBERSECURITY MONTH



WHY
THE
PASSWORD
FUSS?
#CSM2019

My password's been hacked again.
That's the third time I've had to
rename the dog.

Never say
“That won’t happen
to me.” Life
has a funny way
of proving us
wrong.

<https://haveibeenpwned.com/>

HOW SECURE IS MY PASSWORD?

●●●●●●●●●●●●●●●●●●

SHOW SETTINGS

It would take a desktop PC about
178 quadrillion years
to crack your password

[Tweet Result]

HIDE DETAILS

Length: 18 characters

Character Combinations: 81

Calculations Per Second: 4 billion

Possible Combinations: 22 decillion

<https://howsecureismypassword.net>

Password Security



Do not hand your password over to anyone, ever!



Always use different passwords for all your different accounts



Make your passwords long and strong



Never use personal details for your password



Change your passwords regularly



Never leave it lying around



CYBERSECURITY MONTH



HANDY
TOOLS TO
KEEP YOUR
PASSWORDS
COOL
#CSM2019



CYBERSECURITY MONTH

ONLINE
AND
OFFLINE
SAFETY

#CSM2019





FaceApp was a test. We didn't pass

Commentary: Our inability to draw lines when it comes to our personal data is a real problem, with real ramifications. This won't age well.

BY RY CRIST | JULY 19, 2019 7:08 AM PDT



I woke up, poured some coffee and, as I often do each morning, checked Twitter. There, among the headlines, were faces. [Old faces, young faces, weird faces.](#) Altered faces of friends, colleagues and strangers, all of them using [FaceApp](#), the [latest viral trend](#). God forbid we miss out on any of those.

"Why on earth are you still tweeting FaceApp pics?" I asked one of them. This



FaceApp lets users upload a picture, then alter it to look older, younger or like another gender.

Sarah Tew/CNET

A Pokemon Go malware app was downloaded by half a million people

By Patrick Goss September 15, 2016 Mobile phones

Sophisticated Trojan picked out its favored victims



Pikachu does not approve

[Techradar 2016](#)





csirt@uct.ac.za



csirt.uct.ac.za