NELSON MANDELA UNIVERSITY

Cyber Safety and Digital Well-being

Prof Kerry-Lynn Thomson

7 January 2026

A Day in the Life of the Internet

Digital Around the World

Total Population	Internet Users	Active Social Media Users
8.2 BILLION	5.56 BILLION	5.24 BILLION

Source: HootSuite; We are Social

Overview of Global Internet Use

Total Number of Global Internet Users	Internet Users as Percentage of Total Population	Annual Change in the Number of Global Internet Users	Percentage of Users Accessing the Internet via Mobile Devices
5.56 **BILLION**	**67.9%**	**+2.5%** **+136 million**	**96.3%**

Source: HootSuite; We are Social

South Africa

CRICS
CENTRE FOR RESEARCH
IN INFORMATION
AND CYBER SECURITY

Total Population	Internet Users	Mobile Connections	Active Social Media Users
64.4 MILLION	50.8 MILLION (78.9%)	124 MILLION (193%)	26.7 MILLION (42.8%)

Source: HootSuite; We are Social

Time Spent Online

Average Daily Time Internet Users, aged 16-64 years

CRICS
CENTRE FOR RESEARCH
IN INFORMATION
AND CYBER SECURITY

Average Daily Time Users Spend Using the Internet (Global)

6h38m

Average Daily Time Users Spend Using the Internet (SA)

9h37m

Source: HootSuite; We are Social

Time Spent Online

Average Daily Time Internet Users, aged 16-64 years

CRICS
CENTRE FOR RESEARCH
IN INFORMATION
AND CYBER SECURITY

Time Spent Using the Internet (all devices)

9h37m

Time Spent Watching Television

4h29m

Time Spent Using Social Media

3h36m

Time Spent Listening to Music Streaming Services

2h00m

Time Spent Reading Press Media

1h28m

Time Spent Playing Games on a Games Console

1h13m

Source: HootSuite; We are Social

University Students Internet Usage

CRICS
CENTRE FOR RESEARCH
IN INFORMATION
AND CYBER SECURITY

Students spend large amounts of time online, often well over **8 - 10+ hours** per day

Dominant uses are **social media** and **communication** - more frequent than **study** tasks

Smartphones are the main means of access

NELSON MANDELA UNIVERSITY

Our Interconnected World

CRICS
CENTRE FOR RESEARCH
IN INFORMATION
AND CYBER SECURITY

30 billion devices

40+ billion devices - 2034

> “The more connected we are, the more vulnerable we are”

Andrew McAfee
Principal Research Scientist, MIT

Universities are under attack…

CRICS
CENTRE FOR RESEARCH
IN INFORMATION
AND CYBER SECURITY

Colleges and universities a prime target for cybercrime:

Huge, constantly changing user populations

Open Networks

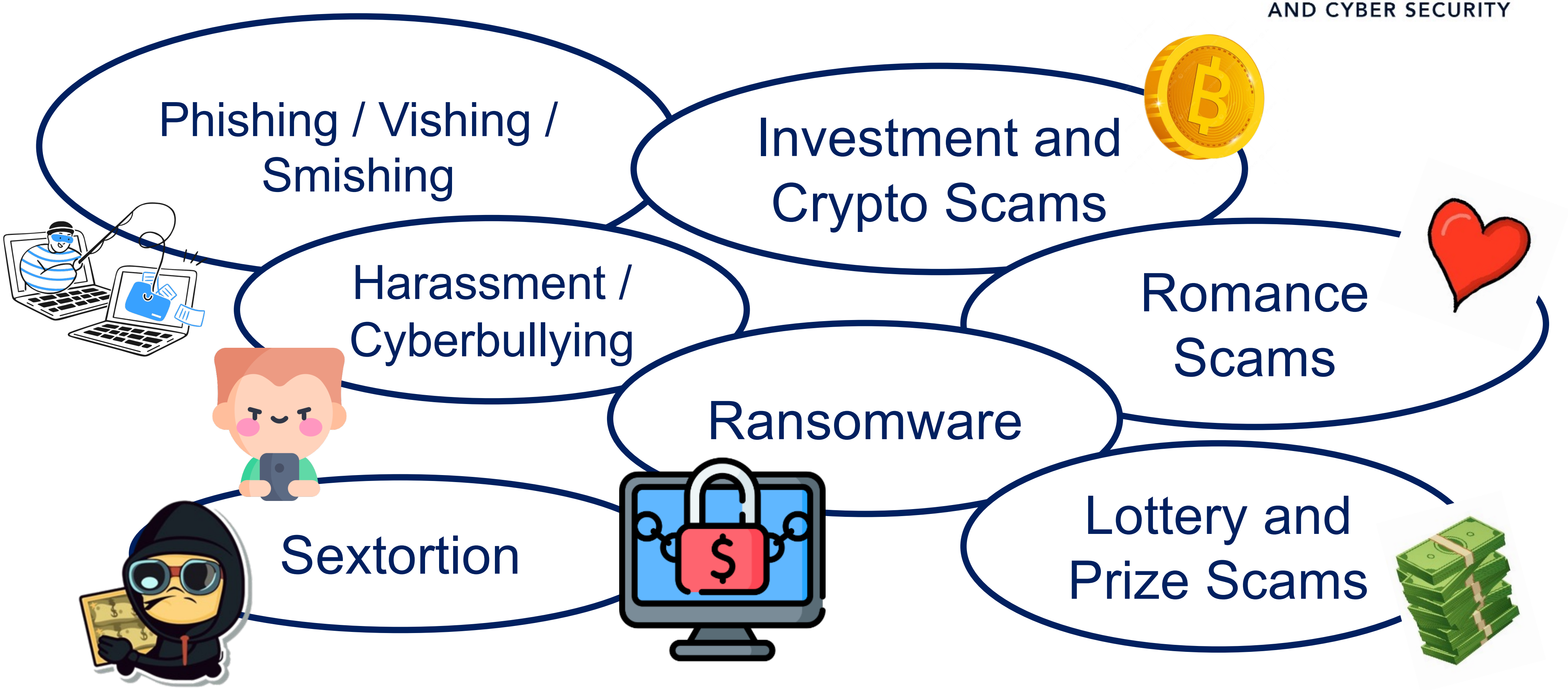
Students are Prime Targets

Limited Cybersecurity Budgets

Valuable Data

Most Common Cyberthreats

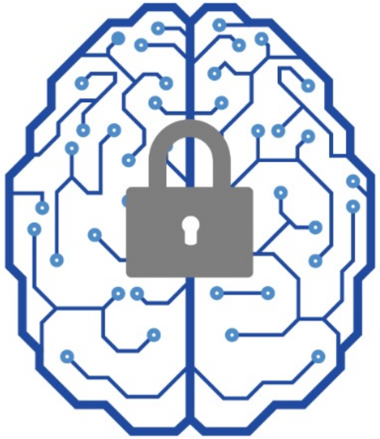
CRICS
CENTRE FOR RESEARCH
IN INFORMATION
AND CYBER SECURITY



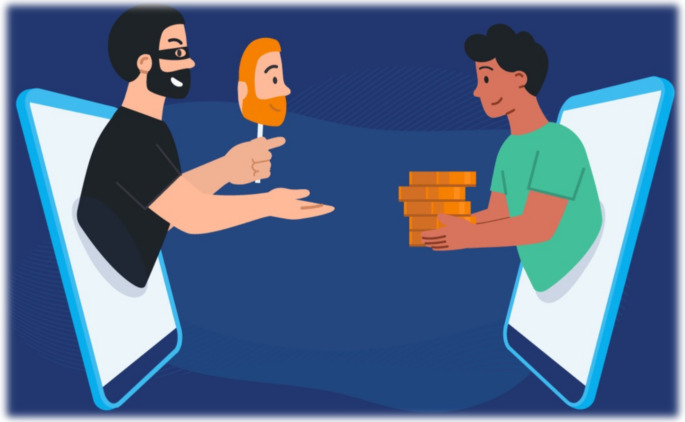
- Phishing / Vishing / Smishing
- Investment and Crypto Scams
- Harassment / Cyberbullying
- Romance Scams
- Ransomware
- Sextortion
- Lottery and Prize Scams

Social Engineering

Influencing people to perform certain actions or divulge **confidential** information



Hacking the Human



National Student Financial Aid Scheme (NSFAS) Scams

CRICS
CENTRE FOR RESEARCH IN INFORMATION AND CYBER SECURITY

Fake NSFAS Allowance Messages:

"Your NSFAS allowance is pending"

"Action required to release funds"

NSFAS Account Verification Scams:

Messages claim the student's NSFAS account is:
'Suspended'; 'Under review'; 'Flagged for non-compliance'

NSFAS
National Student Financial Aid Scheme

Fake NSFAS administrators or "agents":

Scammers pose as:
NSFAS officials; University financial aid staff; "NSFAS consultants"

Accommodation and Landlord Scams:

Fake accommodation listings claim:
"NSFAS-accredited housing"
"Guaranteed NSFAS payment"

Mis/Dis/Mal information…

CRICS
CENTRE FOR RESEARCH
IN INFORMATION
AND CYBER SECURITY

Misinformation

False information that is shared *without* the intent to deceive - often spread by people who believe it’s true

Disinformation

False or misleading information that is deliberately created and shared to deceive or manipulate people

Malinformation

True information that is shared or used with the intent to cause harm

Two Categories of Threat Actors

Cybercriminals and Scammers

Motive: Financial Gain and Making Money

Target Profile: Individuals and Organisations to steal personal, financial and health data that can be monetised (identify theft, fraud, selling on black markets)

Tactics: Phishing, malware and ransomware

Target selection: Indiscriminate, looking for any vulnerabilities to exploit at scale

Propagandists and Disinformation Artists

Motive: Political/ideological motivations, sowing discord and confusion, undermining trust

Target Profile: People’s perceptions, beliefs and behaviours by manipulating the information environment and spreading false narratives

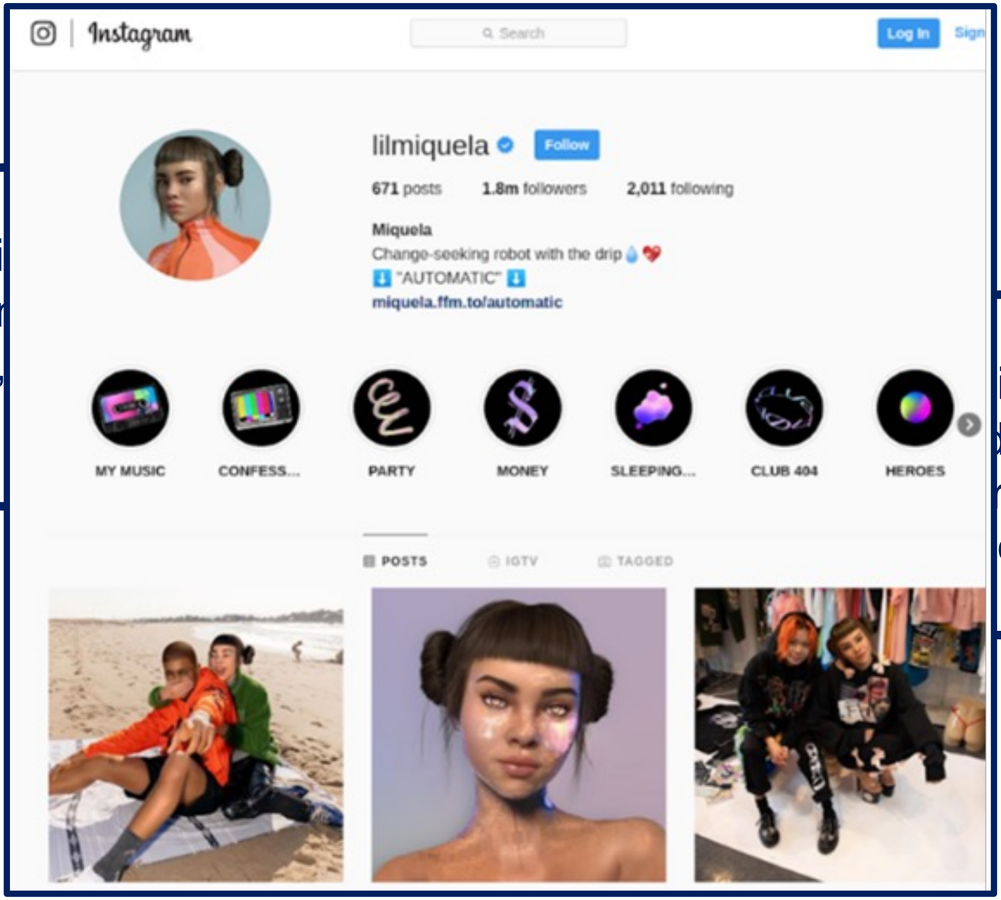
Tactics: Troll farms, bots to flood mis/dis/mal-information and propaganda

Target selection: Aiming information tactics at specific audiences, based on existing beliefs, prejudices and vulnerabilities

Generative AI and Synthetic Media

Generative AI

Type of artifi
can create r
images, music,
data it



lilmiquela

671 posts 1.8m followers 2,011 following

Miquela
Change-seeking robot with the drip 💧❤️
⬇️ "AUTOMATIC" ⬇️
miquela.ffm.to/automatic

Synthetic Media

images, videos,
deepfakes, that is
red using artificial
other digital tools

Generative AI and Synthetic Media

“Generative AI has crashed the party, bringing synthetic media creation to the masses.
It’s like handing a bazooka to someone who used to throw spitballs.”

Perry Carpenter, FAIK

Financial Impact

Losses may include:

Stolen allowances or bursary funds

Drained bank accounts

Credit taken out fraudulently in a student's name

Loss of savings meant for fees, rent or food

For many students:

Even small losses are catastrophic

Recovery options are limited

There is no financial safety net

Could mean choosing between data, food or transport

Psychological Impact

Cybercrime victims often experience:

Anxiety and panic

Shame and self-blame

Fear of exposure

Depression and hopelessness

Loss of trust in online spaces

Students frequently do not report incidents due to:

Embarrassment or stigma

Fear of disciplinary consequences

Belief that they ‘should have known better’

Lack of clarity about where to seek help

Academic Impact

CRICS
CENTRE FOR RESEARCH
IN INFORMATION
AND CYBER SECURITY

Cybercrime and scams interfere with:

Concentration and memory

Attendance and participation

Engagement with online learning platforms

Students may:

Avoid email or LMS platforms

Miss deadlines due to stress or account lockouts

Withdraw from group work and online discussions

When digital spaces feel unsafe, academic participation declines

Further Impacts

Digital Overload

Constant digital **demands**, **notifications** and **information** exceed an individual's **cognitive** and **emotional** capacity, leading to stress, fatigue and reduced effectiveness

Social Media Pressure

Stress and anxiety created by constant comparison, visibility and perceived expectations to present a curated, idealised version of oneself online

Internet Addiction

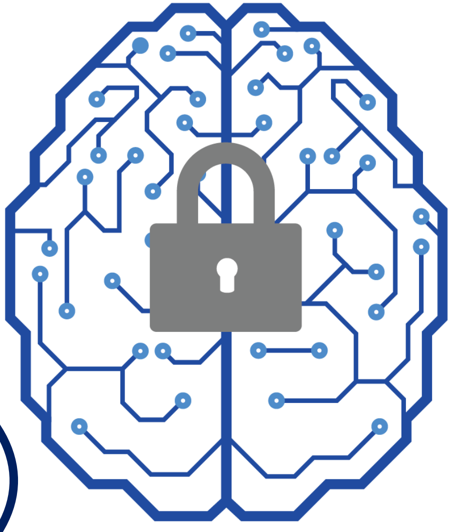
Pattern of compulsive, excessive online use that interferes with daily functioning, relationships, academic performance and mental well-being

Digital Resilience

Ability of individuals to **anticipate**, **cope** with and **recover** from challenges, threats, or disruptions in digital environments, while continuing to engage **safely** and **effectively** online

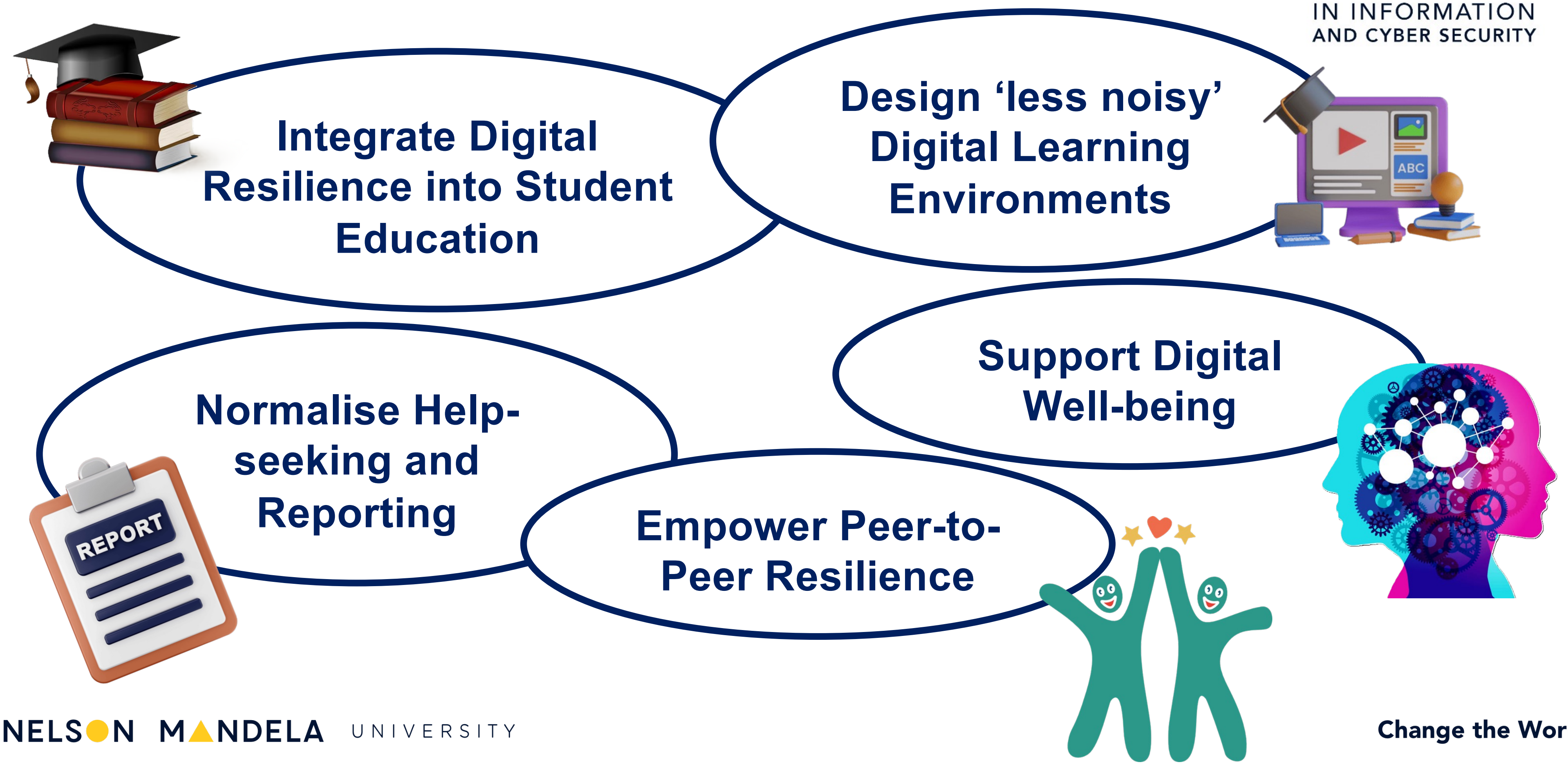
Digital wellbeing

is not about disconnecting entirely - it’s about designing environments that **protect attention**, **dignity**, **safety** and **recovery**



Building Digital Resilience

CRICS
CENTRE FOR RESEARCH
IN INFORMATION
AND CYBER SECURITY



Integrate Digital Resilience into Student Education

Design ‘less noisy’ Digital Learning Environments

Normalise Help-seeking and Reporting

Support Digital Well-being

Empower Peer-to-Peer Resilience

Cyber Safety + Digital Well-being = Digitally Resilient Cyber Culture

CRICS
CENTRE FOR RESEARCH
IN INFORMATION
AND CYBER SECURITY

NELSON MANDELA UNIVERSITY

Change the World

Change the World

mandela.ac.za

Prof Kerry-Lynn Thomson
kerry-lynn.thomson@mandela.ac.za