Province of the
EASTERN CAPE
EDUCATION

OFFICE OF THE DIRECTOR: INFORMATION COMMUNICATION TECHNOLGY
Steve Vukile Tshwete Complex, Zone 6 Zwelitsha, 5608, Private Bag X0032, Bhisho, 5605 REPUBLIC OF SOUTH AFRICA:
Enquiries**: Mr Mfanawethu Cele . Tel: 040 608 4244. Fax :040 608 4672. Email:** mfanawethu.cele@ecdoe.gov.za
Website: www.eceducation.gov.za

Email Protection and Information Security Awareness

Issued by the Office of the Director ICT on 11 February 2022

The Eastern Cape Department of Education have deployed an array of technical countermeasures to protect information and computer systems over the past years. Despite the big investment in technical countermeasures the study conducted over decades in the world have proved that the human remains the weakest link in the information security chain.
New information and communications technologies and COVID-19 have revolutionised work and life in the 21st century. The constant connectivity enabled by digital devices allows work to be performed at any time and from almost anywhere. To safeguard yourself and our organization, the following guidelines are recommended:

Use a strong email password.

- you can use a mix of different characters; ideally, you'll use a blend of lower-case letters, upper-case letters, numbers, and special symbols

Use different email passwords for different email accounts.

- If you use the same password for each account, all your accounts will be compromised if only of them gets infiltrated.

Change your email password often.

- It's also a good idea to change your passwords on a regular basis. Depending on your personal risk factors and how secure you want to be, changing once a year is a good minimum to pursue

Never give out your email password.

- No reputable email company/ organization will ever ask you for your password directly, over email or over the phone.
- If someone is claiming to be a representative from any organization and asks you for your password in one of these communication channels, it's almost certainly a scam

Enable 2-factor / multi-factor authentication.

- The Eastern Cape Department of Education have implemented a 2-factor authentication, sometimes called 2-step or multi-factor authentication
- Essentially, this prompt you for two pieces of personally identifying information before it successfully logs into your account; usually, this means providing a password as well as a temporary passcode sent to your mobile device via text message.
- If this is not activated in your machine, please contact ICT help desk to activate this facility

–Be careful which Wi-fi networks you use.

- Always access your email account only when you're confident in the security of the network you're using.
- For example, it's typically a bad idea to rely on publicly accessible, unsecured Wi-Fi to log into your email; hypothetically, anyone with access to the public Wi-Fi could monitor your actions and gain access to your personal information.
- Therefore, stick to trusted Wi-fi networks

Be aware of email schemes.

- Many scammers rely on email as their medium of choice for operating schemes; email is cheap and infinitely scalable, so it makes sense to them to use emails phishing
- "Phishing," where an email mimics the appearance of a trusted authority (such as your bank, or a major website like eBay) to lure you into giving out personal details, like your credit card number or email password.

Never open an un-trusted attachment.

- Attachments are the most common way to spread malware, which can nab your personal information or even render your machine inoperable.
- Only open attachments in line with your expectations for what an attachment should look like, and from users you trust.
- If you're ever in doubt, call the person who sent you the attachment and ask them to verify its contents

Never give away critical personal information in an email.

- If anyone asks you for your birthday, social security number, credit card number, or password, it's almost certainly a scam.
- Call the company / organization or representative asking for the information by finding that contact info online, not by following the contact information in the email you received and ask them to verify the request.

Avoid replying to scammers and spammers.

- If you've identified a scammer, you might be tempted to respond to them to give them a piece of your mind, or to amuse yourself. However, it's typically better to avoid replying.
- Sending a response will verify that your email address is valid, opening the door to more attacks in the future.

Log out of your email account when finished.

- When you've finished yet another productive day, log out of your email account. This is an especially good practice if you're using an unfamiliar device or a network, you're unfamiliar with, but you should probably adopt it 100 percent of the time.
- This makes it harder for someone to gain access to your email account just by starting your device

Remember: The organization can implement all the technical security hardware and software but "human remains the weakest link in the information security chain" So let us be vigilant to protect ourselves and the organizations that employed us.