



STANDARD BANK GROUP

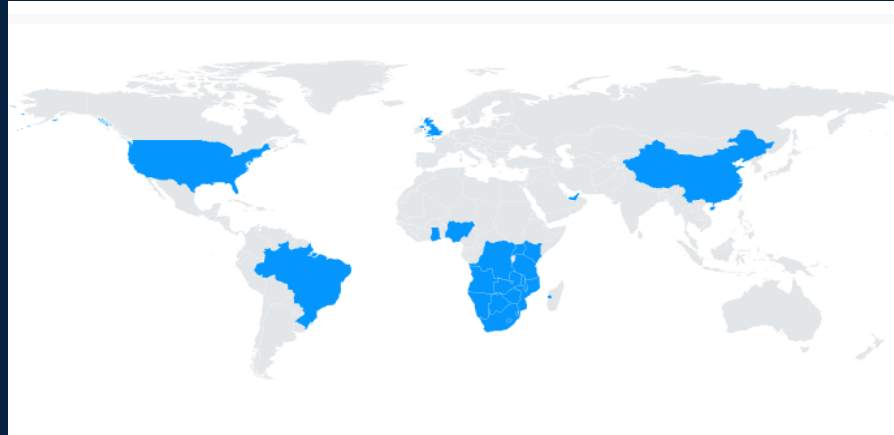
SECURITY AND CULTURE AWARENESS

June 2022

Security Culture and Awareness – Standard Bank Team



Amanda Manzini



Standard Bank footprint

Amanda is the Security Culture and Awareness Manager at a Group level.

She supports the local Culture and Awareness champions across the group in 27 Countries.

There are at least 2 Culture champions per country in Africa. Culture champions in London and Isle of Man support all smaller offices outside Africa



Security Culture and Awareness – Monthly Content

Don't be Phish food - Think before you Click

Group Technology <Itcommunications2@standa...>
To: Pillay, Natasha N (IT Security)

Be security savvy when working from home

Group Technology <Itcommunications2@standa...>
To: Pillay, Natasha N (IT Security)

Don't be phish-food. THINK BEFORE YOU CLICK

Cyber criminals are constantly trying to attack our staff and customers. Social engineering tactics use credentials and personal information, or to click on an attachment.

80% of malicious software attacks are as a result of phishing.

Secure your home network

If you haven't already, update the username and password of your router immediately. Most routers come with default login credentials that are public, which means anyone within range could log in and change settings. Protect your network with a strong, unique password.

INFORMATION SECURITY
Business Email Compromise

IT CAN BE.

Business Email Compromise (BEC) is a highly damaging attack in which cybercriminals use email to target an organisation that they are trying to gain access to. They pretend to be executives, legal, sales, IT, or external vendors; usually someone that is somewhat familiar.

- Their goal is to trick you into giving them the following information or resources:**
- Money
 - Login information
 - Banking details
 - Proprietary information and processes
 - Other sensitive information

BEC attacks attempt to influence and persuade you to take any action that is not in the best interest of your organisation. Cybercriminals approach BEC in four stages:

Don't let social media sabotage your cybersecurity

23 April 2020 02

When opening links on your favourite social media platforms, you don't really think that you will be a victim of cybercrime, but social media just sometimes, to share photos and updates with friends, partners and family? Can a lot of damage really be done through social media?

There are many ways a bad person can target you on these platforms. One tactic that is gaining traction is social media phishing and this can do some real damage.

If you have clicking on one link but are not careful, you could be a victim of social media phishing. A special approach to social media phishing is to use the 'Like' button. This can be used as a credential that will open your internet. You then click on the link in the email or computer and this downloads malicious software to your device or takes you to a page that looks like you're providing more personal details.

The BLUE

Coming soon: The Bank's First Conversational AI

Explore the Future-Ready Transformation learning pathway

100 days of the...

The Blue Edition 13

Group Communication <Marketing Communication@standa...>
To: Pillay, Natasha N (IT Security)

Are you a lover of Jazz? Don't miss your opportunity to attend an online festival!

Do you want to be financially fit?

Can you spot fake news?

3 July 2020 12:18

Fake news spreads like wildfire on social media and is often intended to damage the reputation of a person or entity or make money through advertising revenue.

When looking at a news story on social media, here are some things to look at to determine whether it is fact or fake:

Does the headline match the content?
Read the entire article, the headline may just be used to grab your attention.

Are there spelling or grammar errors?
Legitimate publications often go through layers of editing before content is published. Spelling and grammar errors indicate that the author may not be a professional writer.

Who is the author?
If there is not one listed, it's a red flag. Also, if the author's name is present, do a Google search to see if they are part of a legitimate organisation.

Is there a website?
Does the publication have a website or a social media presence? This offers a full view of a fake news article.

Does the headline seem overly outrageous?
If it seems unbelievable, it probably is. Trust your instincts. If the article you are reading is too good to be true, it probably is.

The Blue Edition 9

Group Communication <Marketing Communication@standa...>
To: Pillay, Natasha N (IT Security)

The BLUE

Check out How personalisation is shaping banking.

Tips to keep your children cyber-savvy

1. Talk to your children about their online activity

2. Keep computers and devices where you can see them

3. Always remember your child's name when using devices

4. Know who your children's online friends are

5. Keep your parental controls

6. As adults, we know that some people will never who they say they are, but children and young people can be starting to see what they are up to when they are not supposed to be. Your children may need to be taught how to spot these people.

7. Make sure you become friends and contacts with your child's social media friends and ensure you monitor posts. Your children may need to be taught how to spot these people.

10 tips to keep your children cyber-savvy

6 June 2020 08:00

In this Digital Age, younger kids are spending more and more time online.

The COVID-19 pandemic has complicated the situation. The children are spending more time online than ever before, and this is often to help them to learn, to play, to socialise and to stay connected with their friends.

As a parent, it's important to make sure your children are safe and secure online. Here are 10 tips to help you do this:

1. Talk to your children about their online activity
2. Keep computers and devices where you can see them
3. Always remember your child's name when using devices
4. Know who your children's online friends are
5. Keep your parental controls
6. As adults, we know that some people will never who they say they are, but children and young people can be starting to see what they are up to when they are not supposed to be. Your children may need to be taught how to spot these people.
7. Make sure you become friends and contacts with your child's social media friends and ensure you monitor posts. Your children may need to be taught how to spot these people.

Security Culture and Awareness Campaigns – Cyber Month



THE BLUE Magazine – Cyber Edition

Hackers are always looking for victims. DON'T BE NEXT!

At Home? Travelling? Or using the Cloud? Avoid Cybercrime with these 20 Tips

So you think your password is strong? Test it with our Password refresher guide

Follow Julia, Mark and Tim make blunders that teach you about staying safe on Social Media

And so much more...

Click here to read Edition 024

IT CAN BE.

At Home? Travelling? Or using the Cloud? Avoid Cybercrime with these 20 Tips

AT HOME

20 Ways to Block Mobile Attacks

Let's go "Phishing" for red flags

REPORT (PHISH)

CONTENT

ATTACHMENTS

HYPERLINKS

IT CAN BE.

Yammer Campaign

PASSWORD SECURITY TIPS

Use multifactor authentication (MFA) where possible to protect valuable data and content.

PHISHING AWARENESS TIPS

Make sure you read the full email address of the sender. If the email address looks suspicious, report it.

IT CAN BE.

Stream Campaign

HOW WOULD YOU REACT TO YOUR EMAILS BEING HACKED?

Well, we conducted an experiment with a few of our colleagues. They were duped into thinking their email addresses were "hacked" and they were being impersonated via email. We recorded their reactions.

Cyber criminals are constantly looking for their next victims and anyone of us can be next if we Take the Bait. Don't get caught out like our colleagues were in this experiment.

Click here to listen to their reactions

IT CAN BE.



Building CYBER Security Skills In and For Africa

987 **ENTER**
Employees that heeded the call and signed up to tackle the CSA entrance challenge.

75
Graduates completed the program with **6** from Africa Regions and **8** from Liberty.

15%
of graduates have already been hired into IT Security with more planned.

Program included **5** modules:
CTF, Core Security, Security Engineering, Cyber Security and Vendor Training.

The whole programme ran for **5** months.

200 Hours of after-hours work required to complete the full program.

10 Africa Regions countries that were represented in the program.

4 Industry recognised certifications from: AWS, Forcepoint, Cybereason and IBM.



Standard Bank

The shortage of skilled Cyber Security staff across the Group led to the development of the Standard Bank Cyber Security Academy. The program was developed through the expertise of the Group IT Security team in collaboration with our strategic partners. The training was designed to give participants incredible opportunities to future proof their skills, increase their knowledge base and expand their career options.

All those who undertook this journey, got to test their problem-solving skills, gained security knowledge, got exposed to industry accredited certifications and collaborated with like-minded, dynamic individuals across the Group. **To the class of 2019, we once more say, congratulations and keep challenging yourself. We look forward to continuing the effort to achieve our goal of "Building Cyber Security Skills In and For Africa" in 2020.**

