

Changing Security Culture

Best Practices what works, what doesn't..

Anna Collard
Managing Director
KnowBe4 Africa – formerly
Popcorn Training

About KnowBe4

KnowBe4
Human error. Conquered.



- Integrated new-school Security Awareness Training and Simulated Phishing platform
- Head Office based in Tampa Bay, Florida, founded in 2010.
- Rated as a leader by major analysts
- KnowBe4 Africa based in Cape Town & Joburg





Anna Collard

Managing Director KnowBe4 Africa

About Anna

- CISSP, CISA, ISO 27001 Lead Auditor & Implementer, FTI Business Analyst, (ex)PCI DSS QSA, (ex) CIPP/IT; BA international economics,
- Founder (2011) of South Africa based Security Awareness content publisher Popcorn Training – now a KnowBe4 company.
- Mum of 2, Wife

Agenda

- 6 Security Awareness – best practices
 - Executive Buy In for SAT
- Keeping engagement
- Showing Return of Investment / metrics
- What's coming soon..

Worst Practices

- Or what doesn't work...

Annual Awareness Sessions... (if that's the only thing..)



Monthly Security Videos...



Sporadic Phishing Simulation



Why Is Getting the Desired Behaviors So Difficult?





You can't effectively train on everything...

If your goal is behavior change,
focus on 2 to 3 behaviors at a time

The “Magic Wand” Thought Experiment

If you could wave a magic wand and instantly change three security behaviors in your organization, what would they be?

Changing Security Cultures



1. **Gain executive buy in & involvement**
2. **Get baseline metrics & set explicit goals**
3. Comprehensive, **co-ordinated** campaigns
4. **Relevant** short, interactive content
5. Avoid **cognitive overload**
6. **Combine with random frequent** simulated phishing attacks

Changing Security Cultures



1. **Gain executive buy in & involvement**
2. Get baseline metrics & set explicit goals
3. Comprehensive, **co-ordinated** campaigns
4. **Relevant** short, interactive content
5. Avoid **cognitive overload**
6. **Combine with random frequent** simulated phishing attacks

Know Your Scope of Influence..



Culture is led from the **very** top of the organization; it doesn't originate from IT or Security.

1. Get Executive Involvement

- Awareness starts at the top
- Ask for Involvement beyond just paying for it
- Use statistics & facts → Return on risk reduction



Phishing Still Remains No 1 Threat Action

2019 Data Breach Investigations Report

verizon
business ready

*Verizon Data Breach report 2019
<https://enterprise.verizon.com/resources/reports/dbir/>

Phishing was involved in

- **32%** of confirmed breaches

Other causes:

- 28% malware infections,
- 29% use of stolen credentials—

ROI of Security Awareness Training?

Reduce risk of infection caused by human error down to 10%

Figure 7
Larger Organizations, Annual Cost per Employee

| | Before SAT | After SAT | ROI |
|--------------------------------|-----------------|-----------------|------|
| Disinfecting workstations | \$5.28 | \$4.63 | 562% |
| Remediating malware/ransomware | \$483.52 | \$48.35 | |
| Labor cost of SAT | \$0 | \$11.90 | |
| Cost of SAT | \$0 | \$17.50 | |
| Employee time spent on SAT | \$0 | \$27.83 | |
| TOTAL | \$488.80 | \$110.21 | |

Source: Osterman Research, Inc.

*The ROI of Security Awareness - Osterman Research 2019

– <https://www.computerworld.com/resources/197650/osterman-research-the-roi-of-security-awareness-training>

African Cyber Security Awareness Stats

- 28% fell for a **phishing** email
- 27% fell for a **scam** / con artist
- 50% had a **malware** infection
- 65% are concerned about cybercrime
- 28% don't know how to protect themselves
- 55% confident they recognize a security incident



65% don't know what ransomware is

52% don't know what multi-factor authentication is

**KnowBe4 Africa Cyber Security Survey Nov 2019 – 800 respondents across South Africa, Nigeria, Kenya, Mauritius, Ghana, Egypt, Morocco*
<https://info.knowbe4.com/african-cybersecurity-research-report>

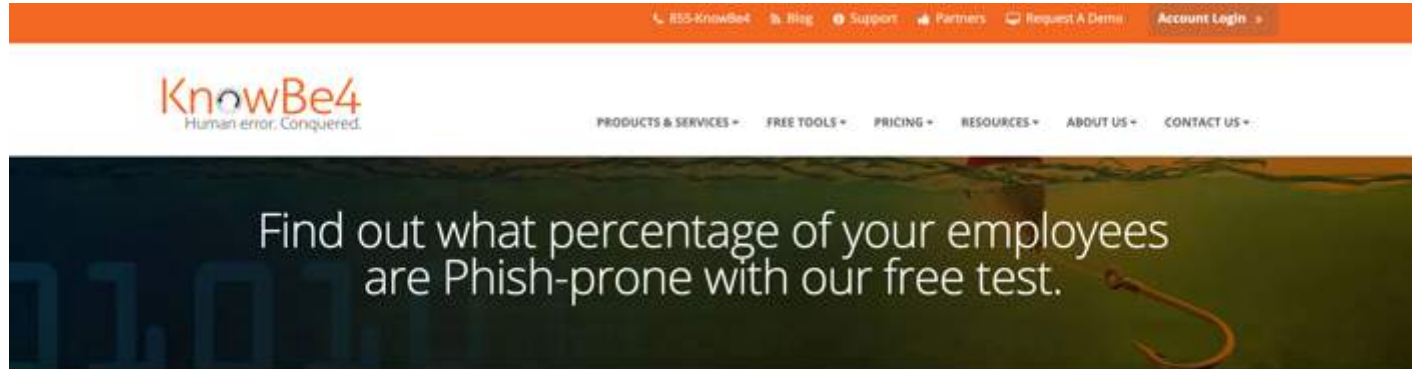
Changing Security Cultures



1. Gain executive buy in & involvement
2. Get **baseline metrics & set explicit goals**
3. Comprehensive, **co-ordinated** campaigns
4. **Relevant** short, interactive content
5. Avoid **cognitive overload**
6. **Combine with random frequent** simulated phishing attacks

2. Define (baseline) metrics & set explicit goals

1



2



2. Baseline metrics & set goals

Example OKRs for Awareness Projects

Bonus:
awareness Sessions at
secretaries' days

OBJECTIVES Set out Jan 2019

1. Improve Phishing Awareness

2. Increase Security awareness coverage

3. Innovate:

Changing Security Cultures



1. Gain executive buy in & involvement
2. Get baseline metrics & set explicit goals
3. **Comprehensive, co-ordinated campaigns**
4. Relevant short, interactive content
5. Avoid cognitive overload
6. Combine with random frequent simulated phishing attacks

3. Co-ordinated Campaign Fit into the Organisational Culture

CULTURE

- Work with HR
- Work with Marketing & communication
- Different cultures in different teams (i.e. IT vs finance)



3. Coordinated Campaign – branding



Play our Tweet or Delete game...
and learn more about the social media posts that have gotten employees into trouble before.



Stand a chance to win...
a pair of JBL Bluetooth earphones.



How?
Check your inbox for notifications from the Cybersmart Team or click on the "Tweet or Delete" banners on the Intranet.



Sanlam | Personal Finance | Life | Investments | Insurance

so you're a clicker?

What next?

Because you clicked on one of our phishing simulations you will be enrolled in remedial training.
Don't panic, the training is short and won't take up much of your time, but it is vital to us that you can identify the key identifiers of a phishing email.

| | | |
|--|--|---|
| 01 mismatched and misleading information | 02 use of urgent or threatening language | 03 promises of attractive rewards |
| 04 requests for confidential information | 05 unexpected emails | 06 suspicious attachments |

We will be testing you again, so make sure that you check for these tactics with each and every out of the ordinary email you receive.

Believe it or not, we want you off that Clickers list soon!

stop. look. think **secureit**

Changing Security Cultures



1. Gain executive buy in & involvement
2. Get baseline metrics & set explicit goals
3. Comprehensive, co-ordinated campaigns
4. **Relevant short, interactive content**
5. Avoid cognitive overload
6. Combine with random frequent simulated phishing attacks

4. Relevant Content – make it personal

We change...

- If it affects family or money
- Doing the “right thing”
- If we “feel” it



4. Personally relevant information

1

QUIZ ANSWERS

THE CYBER MAZE:

WORD SEARCH:

SPOT THE BAD GUY:

CROSSWORD PUZZLE:

CHATTERBOX ANSWERS:

1. Parakeet (the wrong primary settings will mean you lose your personal information)
2. No, Walter downloaded them from the app store. (downloaded from the app store)
3. Yes, an adult (parent/teacher) at school and must be aware of the app.
4. No, because when you post, the app reports cyber safety.
5. Parakeet (Walter got a photo of the first letters of the clue and it was a guess. For example, 'the bird has been in the room' - parakeet - 'Mighty!')

OLD MUTUAL

OLD MUTUAL

THINK BEFORE YOU CLICK!

EPIC CYBER HERO HANDBOOK

Join our league of crime fighting Cyber Heroes!
Every hero needs a helping hand sometimes, so don't be scared to ask your parents.

OLD MUTUAL

DO GREAT THINGS EVERY DAY

THE COVID-19 OUTBREAK: WHAT YOU NEED TO KNOW

A HANDFUL OF INTERESTING FACTS...

1 What is it?

The new coronavirus known as Covid-19 is a respiratory disease that was first identified in Wuhan in China at the end of 2019.

2 Why is it causing worldwide alarm?

In the two months since its outbreak, it has spread to all the continents except Antarctica, causing more than 3 137 fatalities worldwide.

3 How many people have been infected?

As of the 3rd of March there have been more than 90 000 reported cases, but there could be many more unreported cases in countries and regions that have not tested on a large scale.

NO VACCINE has been developed and approved yet

4 Where are the current known high risk areas outside China?

South Korea, Iran and Italy

5 What are the symptoms?



6 What is the fatality rate?

The fatality rate for those infected is between 3% and 4%, which is higher than ordinary flu (0.1%) but far less deadly than the dreaded Ebola virus (90%).

7 Who is most at risk?

It is considered highly contagious and anybody can contract it, but the risk of dying from it is greatest for the elderly and those with weak immune systems.

8 How long is the incubation period?

It's up to 3 weeks, and you can infect others even before you display symptoms and become ill.







Changing Security Cultures



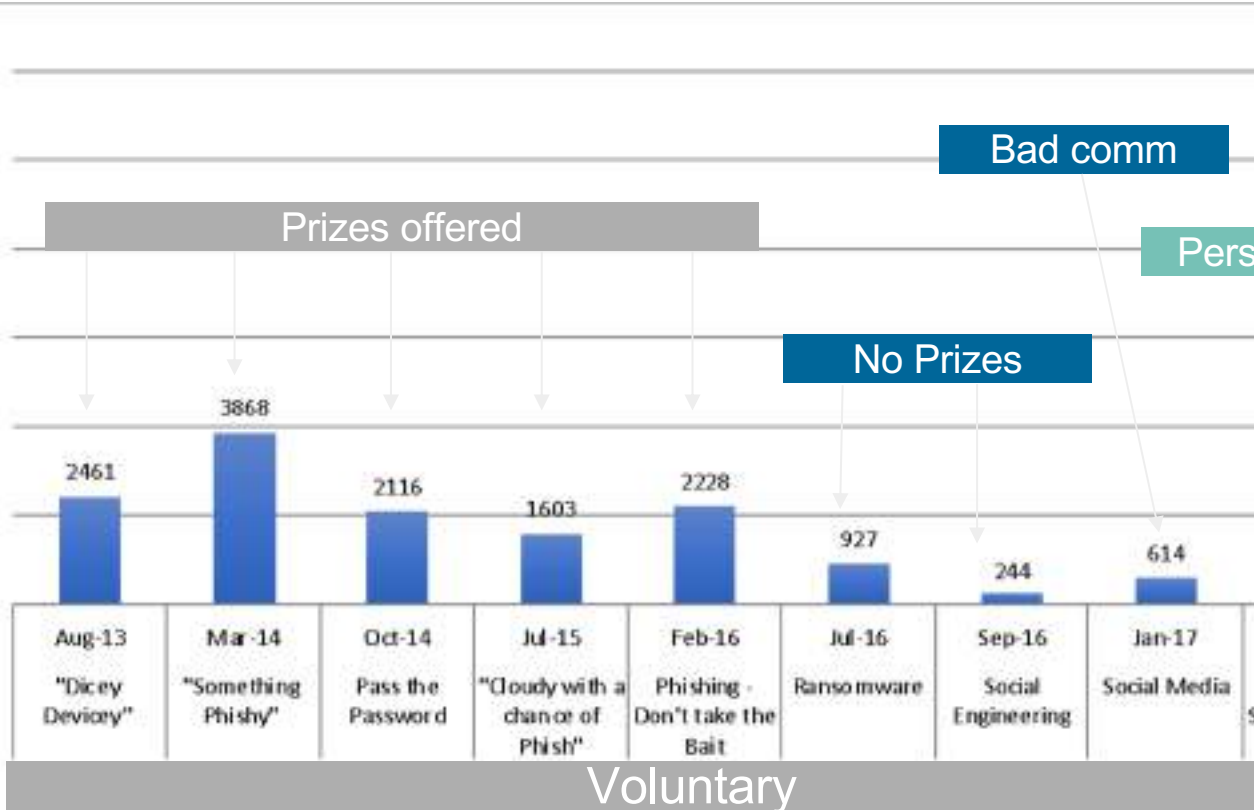
1. Gain executive buy in & involvement
2. Get baseline metrics & set explicit goals
3. Comprehensive, co-ordinated campaigns
4. Relevant short, interactive content
5. Avoid **cognitive overload**
6. Combine with random frequent simulated phishing attacks

5. Avoid cognitive overload

Don't do too much.

| January | February | March | April |
|--|---|--|---|
| <p>TPRM: "Doing the right thing" (Moodle Platform)</p>  <p>On-going Monthly Phishing Simulation</p> | <p>Targeted Training: Managers Cloud Security</p>  <p>On-going Monthly Phishing Simulation</p> | <p>Social Media Game: Tweet OR Delete</p>  <p>On-going Monthly Phishing Simulation</p> | <p>Compulsory E-Learning Training: All Users SIS Policy</p>  <p>On-going Monthly Phishing Simulation</p> |
| September | October | November | December |
| <p>Targeted Training: Secretary's Day</p>  <p>On-going Monthly Phishing Simulation</p> | <p>Cyber Security Awareness Month</p>  <p>On-going Monthly Phishing Simulation</p> | <p>On-going Monthly Phishing Simulation</p> | <p>On-going Monthly Phishing Simulation</p> |

PARTICIPATION STATS



Changing Security Cultures



1. Gain executive buy in & involvement
2. Get baseline metrics & set explicit goals
3. Comprehensive, co-ordinated campaigns
4. Relevant short, interactive content
5. Avoid cognitive overload
6. **Combine with random frequent simulated phishing attacks**

6. Making People Feel: Phishing Simulations

- Frequent
- Randomized
- Increase difficulty level
- Teach red flags
- Make it easy to report



6. Best Practices Phishing Simulations

1. Communicate
2. Automate.. 30 – 50 templates for the year
3. **No South African brands / block outgoing**
4. Get approval
5. Create good landing template(s)
6. **Every 2 weeks or monthly minimum**
7. **PhishAlert button**
8. **Random- random**
9. Monthly metrics



6. Every notification is a chance to communicate with your users: Make it count



Ooops ...

... to protect our chicken, be careful
with that chicken' Andy!

You've just clicked on a potentially dangerous phishing email.

Not to worry though, this email is just part of a simulation exercise being run within Nando's to help raise our awareness and understanding of the sort of cyber threats we face ... so no harm done this time!

If you've got a minute though, hover over the red flags below to see the tell-tale signs you might have spotted:

From: IT <IT@nandosgroup.com>
Reply-to: IT <IT@nandosgroup.com>
Subject: [Change of Password Required Immediately](#)

We suspect a security breach happened earlier this week. [In order to prevent further damage, we need everyone to change their password immediately.](#)

[Please click here to do that](#)

[Change Password](#)

Please do this right away. Thanks!

Sincerely,
IT

Suspect fowl play?

REPORT IT or DELETE IT ... but NEVER take the requested action!

Ooops!
You could've just given away more than chicken!

You've just clicked on a potentially dangerous phishing email. Not to worry though, this one was sent out by Nando's to help raise our cyber security awareness.

How to spot a phish?

Look out for any email that:

- Triggers an EMOTION such as sympathy or fear
- PRESSURES you to take action quickly
- Contains bad SPELLING or is poorly worded
- Is something that you're NOT EXPECTING

What might it ask?

It might ask you to:

- CLICK on a link to a website
- DOWNLOAD or OPEN an attachment
- Provide some PERSONAL or SENSITIVE information (e.g. your password)

What to do?

If you're suspicious:

- CHECK with the sender via phone or text
- LOOK at it more closely
- REPORT it to the Helpdesk

Suspect fowl play?
REPORT IT or DELETE IT ... NEVER take the requested action!

To protect our chickens,
be careful where you're chicken!

Engagement over time... ROI

Training Stats

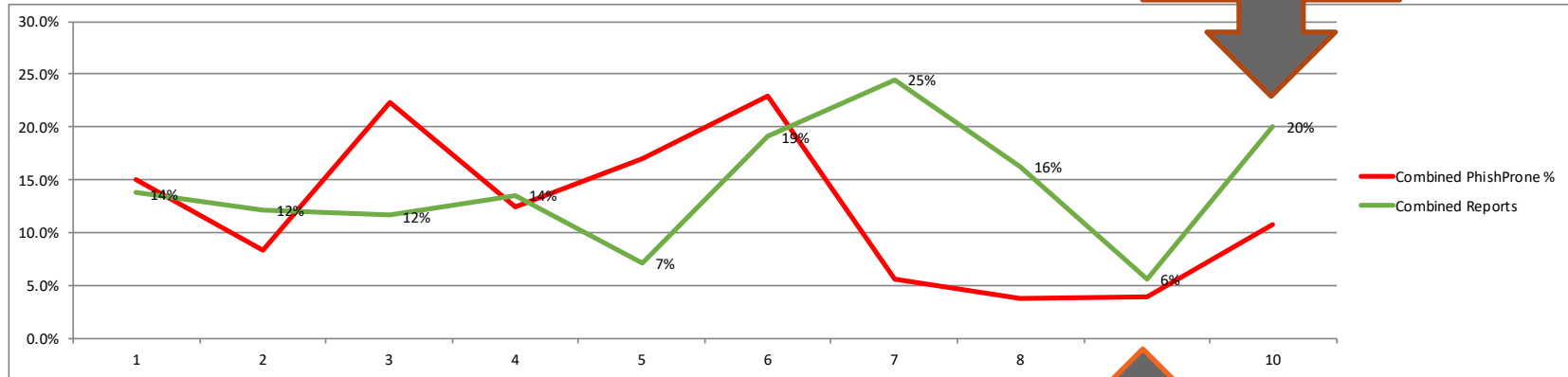
PAN Africa



| | | | | |
|--|--|--|----------------|---|
| In Progress Doing the Right Thing - Rwanda Soras AG 10/09/2019 - (No End Date) | Rwanda - Soras AG | Doing the Right Thing Sanlam Group Policy: Social Media for Individuals | 97% | ▼ |
| In Progress Doing the Right Thing - Rwanda Soras VIE 10/09/2019 - (No End Date) | Rwanda - Soras VIE | Doing the Right Thing Sanlam Group Policy: Social Media for Individuals | 91% | ▼ |
| In Progress Doing the Right Thing - Botswana 10/01/2019 - (No End Date) | Botswana | Doing the Right Thing Sanlam Group Policy: Social Media for Individuals | 84% | ▼ |
| In Progress Doing the Right Thing - Tanzania General 10/01/2019 - (No End Date) | Tanzania General Insurance | Doing the Right Thing Sanlam Group Policy: Social Media for Individuals | 97% | ▼ |
| In Progress Doing the Right Thing - Tanzania Life 10/01/2019 - (No End Date) | Tanzania Life Insurance | Doing the Right Thing Sanlam Group Policy: Social Media for Individuals | 100% Completed | ▼ |
| In Progress Doing the Right Thing - Kenya 10/01/2019 - (No End Date) | Kenya | Doing the Right Thing Sanlam Group Policy: Social Media for Individuals | 96% | ▼ |
| In Progress Doing the Right Thing - Uganda General 10/01/2019 - (No End Date) | Uganda General Insurance | Doing the Right Thing Sanlam Group Policy: Social Media for Individuals | 100% Completed | ▼ |
| In Progress Doing the Right Thing - Mozambique 10/01/2019 - (No End Date) | Mozambique | Doing the Right Thing Sanlam Group Policy: Social Media for Individuals | 78% | ▼ |
| In Progress Doing the Right Thing - Zambia 10/01/2019 - (No End Date) | Zambia | Doing the Right Thing Sanlam Group Policy: Social Media for Individuals | 87% | ▼ |
| In Progress Botswana Doing the Right Thing - Test 08/14/2019 - (No End Date) | Botswana Do the Right Thing Test Group | Doing the Right Thing | 100% Completed | ▼ |

Showing ROI

Graphs always need context



Increased
difficulty level

Easy difficulty level
“Black Friday sale”
Seen as spam – low
reporting

Desired trend behavior:

Phish prone % decrease
Reporting % increase

Keeping Engagement? Gamification, fresh content

Sanlam Life Insurance Leaderboard

See how your group ranks below. Improve your group's rank on the leaderboard by completing all your training assignments.



| Rank | Name | Percentage Complete (%) |
|------|----------------------------------|-------------------------|
| 1 | PAM Your Group | 86% |
| 2 | SEM | 79% |
| 3 | Glacier 2019 | 74% |
| 4 | Sanlam Personal Finance | 73% |
| 5 | Group Technology and Information | 73% |
| 6 | SKV | 71% |
| 7 | Sanlam South Africa | 66% |
| 8 | Group Office | 60% |
| 9 | SIG Sanlam Investment Group | 63% |

Your Achievements

Good work, Cyber Hero. You have earned 6 badges! Check out your heroic achievements below and find out how you can collect more badges.






Tweet or Delete

Start

GAME
Tweet or Delete

Popcorn Training
SIVICS



Debbie Jacobs
@debbie Jacobs

I hate working here... feels like we have dial up internet... what is this? 2006?

Buttons: Reply, Retweet, Like, Tweet

Buttons: Tweet, Delete, Hint



Mike Jones
in Kloof Street Cape Town

Mike Jones
My new colleague...
Rough day at the office?
#WorkSux
Now

Liked by Darrell Shabalala and 34 others
3 DAYS AGO
Add comment Post

Buttons: Tweet, Delete, Hint

What's coming soon?

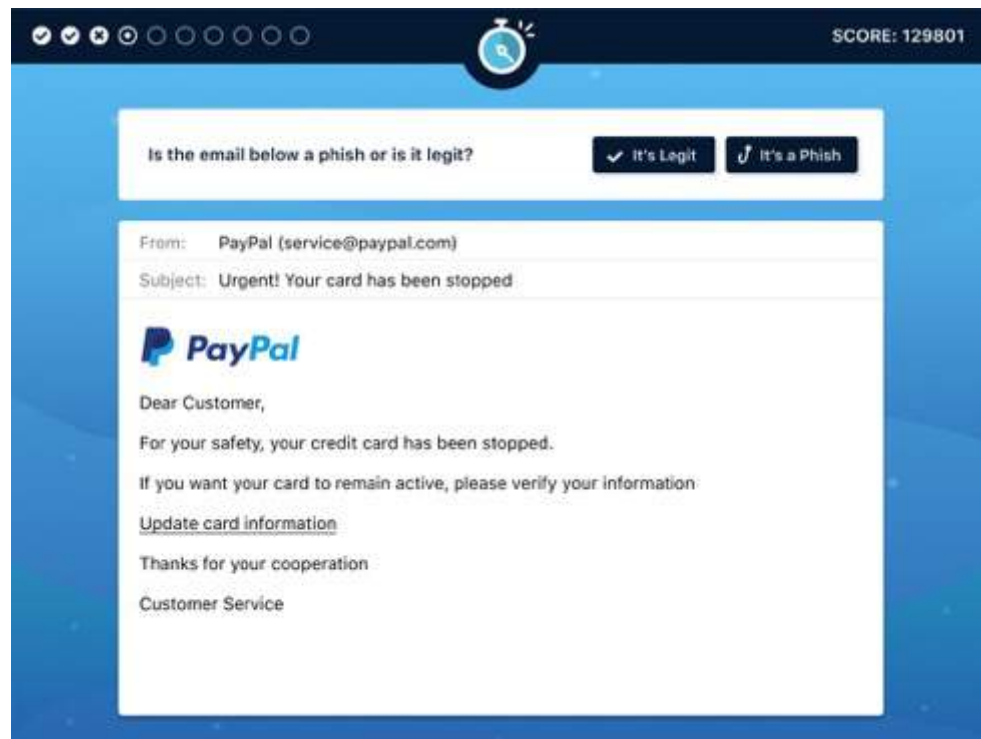
Content:

- Spot the Phish reloaded
- Working from home – safely. (Coronavirus)
- “How to” explainers
- Gauthrain breach story

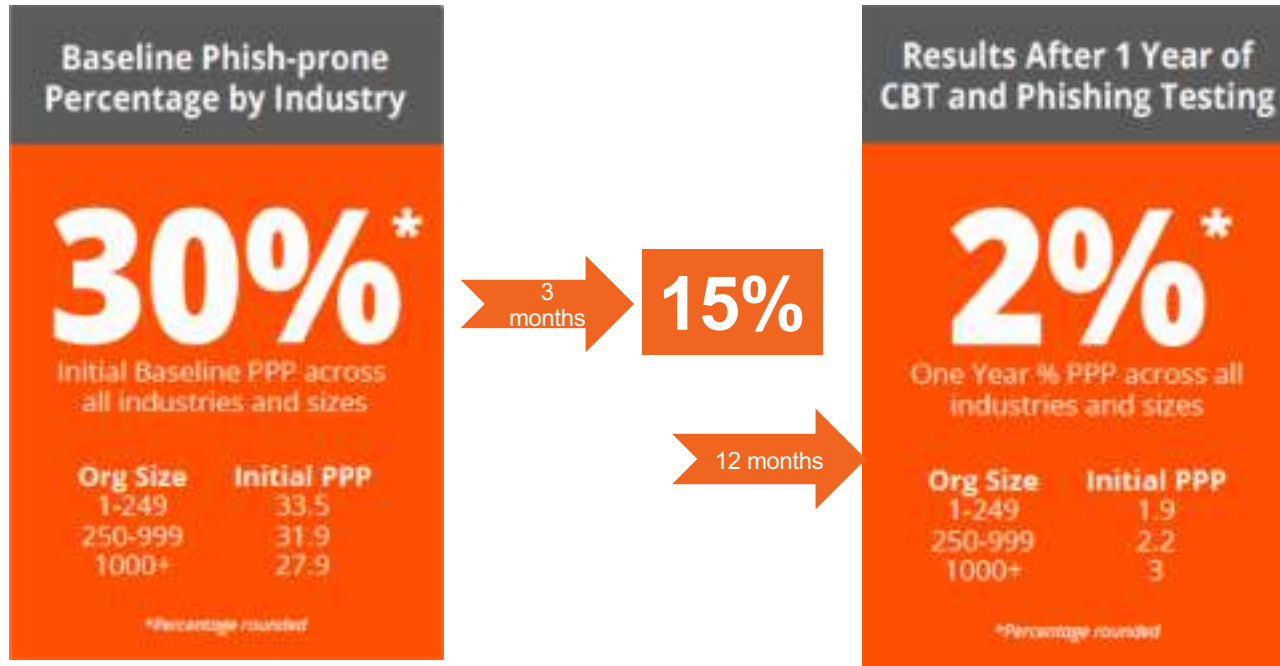
Functionality:

- Branding of content
- PhishRipper – integration into Office365

•



KnowBe4 2019 Phishing by Industry Benchmark Report




In Summary – just do it – and then do it again..



- Work with Marketing & Communications & HR
- **Use short & engaging** content
- Mix it with **personal messages (not always about company)**
- Power of gamification
- Frequent random **phishing simulations**
- **Management Reporting** to show ROI
- Have **fun**

Awareness is a bit like **flossing** – it's an ongoing process

KnowBe4AFRICA
Human error. Conquered.

Formerly known as  Popcorn
Training

Thank You

Get in touch on LinkedIn:

- Anna Collard