AQUILAI
CYBERINTELLIGENCE

Gone Phishing for your credentials…

Spear Phishing

Whale Phishing

Deep Sea Phishing

Zero Day attack

Brand Impersonation

People Impersonation

Phishing is typically impersonation of a person or brand

An attackers' most common entry point into your customers' systems

Credential theft is the objective

Phishing is not Malware or SPAM although they often coincide

86% of data breaches are linked to phishing

UK Government (Department for Digital, Culture, Media & Sport)
Cyber Security Breaches Survey - March 2020

Up until a few years ago, cybercriminals focused their efforts on malware attacks because they provided the greatest ROI. More recently, they've shifted their focus to phishing attacks (~70%) with the goal of harvesting user credentials.

Microsoft Digital Defense Report - Sept 2020

SANS

On average, it only takes 82 seconds from the time a phishing email is first distributed until the first victim is hooked

Cyber Research Databank

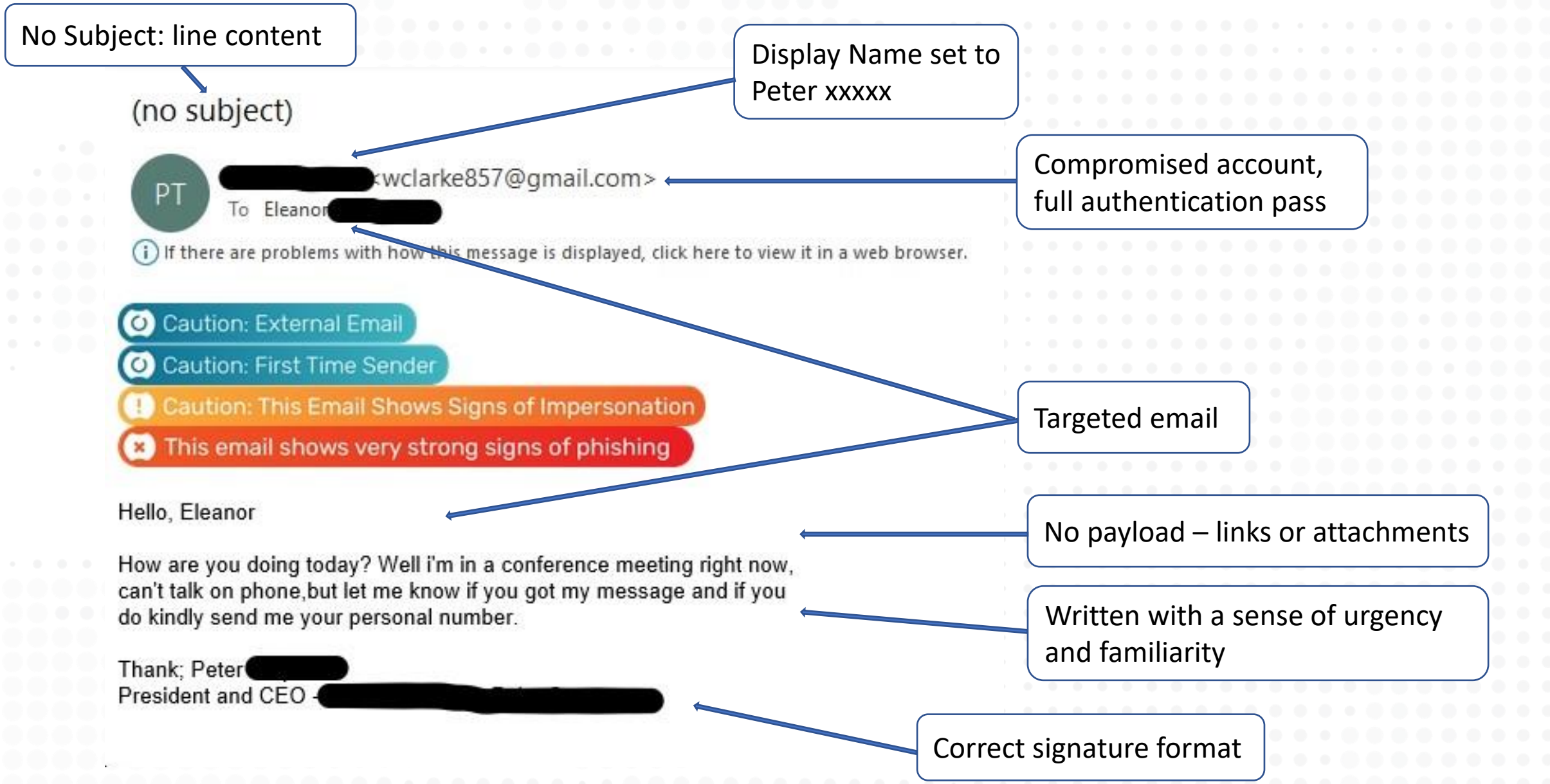
Google & facebook

Each was tricked out of **$100M** by one cyber criminal

Highly profitable for bad actors

Existing phishing solutions – Do Not Work

- 99% of Enterprises already have email filtering deployed
- Gartner state "Do not depend upon a vendors native defenses"
  - Microsoft 365 Advanced Threat Protection (SPAM, Malware & Phishing)
- NCSC state "Phishing education alone is not strong enough"



Impersonation Attack

Leverage latest advances in knowledge

Shaped and guided by UK GCHQ & NCSC

Architected to protect against both current & future attacks

UK Cloud based subscription service

Integrate easily with any cloud based email

Co-exist with deployed security solutions

No updates required, deploy and forget

Effective across all mail clients and devices as no new software required

Existing solutions not working

Totally new approach …

- ✓ Automatic profiling of user organisation for Threat Intelligence
- ✓ Automated User profiling to protect each user
- ✓ Technical analysis determines the source and hidden content
- ✓ Linguistic analysis to determine sentiment, emotive and coercive content
- ✓ Auto learn as attacks change

Phishing Nirvana

Ajax i

to identify user

Stop

OK

Catch Up ?

info@askiconsult.com
Tue 07/05/2019 20:03
Mr Phish

Caution: External Email
Caution: First Time Sender

Dear Mr Phish,

Thanks for checking out the servic

When would you be available for

Regards,

Jim Smith
ASKI Consulting

We've suspended your Netflix account

NETFLIX
Tue 07/05/2019 19:17
Mr Phish

Caution: External Email
Caution: This email contains topics of a financial nature
This email shows very strong signs of phishing

NETFLIX

Your account has been suspended

Dear client,

We've temporarily **suspended** your account due to issues in the automatic verification process.

You will not be able to access your account until you **verify** your identity and update your payment method. We will provide you with all the steps you need to unlock your account. Please follow these instructions after you click on the link below.

UPDATE YOUR DETAILS

Follow these steps :

1. Login to your account.
2. Update your **Billing** information.
3. Update your **Payment** method.

If you do not verify your account, your account will be permanently deleted.

Please help us to validate and unlock your account.

Thanks,

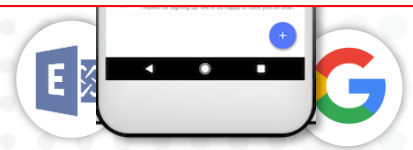
Netflix

ount

topics of a financial nature
g signs of phishing

been suspended

our account due to issues in the automatic verification



AQUI

Reasons for phishing

A link in the email appears to be Imitating a well known company or brand

A link in this email shows signs that the link is impersonating netflix:nznetflix-issue-solve2019.azurewebsites.net. They are attempting to make you believe that the link belongs to a different organisation. Always check the link carefully to ensure that you know where it is going.

The wording of this email is suspicious

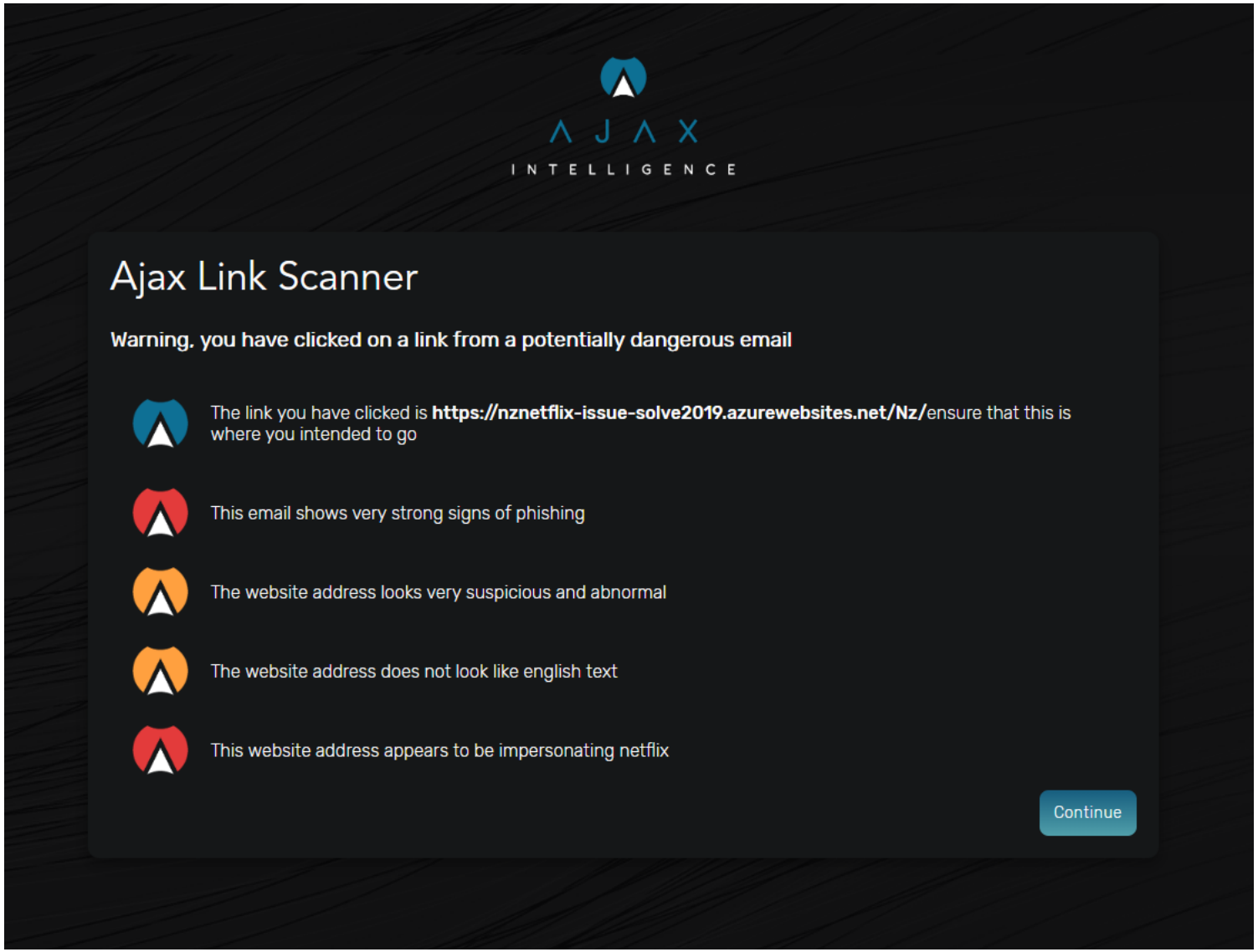
The wording in this email looks similar to the wording commonly used in phishing emails. This could be the sender is attempting to manipulate you into performing an action.

There are links in the email which look suspicious

There are links in the email which have strong features associated with phishing links. This could be that the link is trying to hide its true destination.

This email contains language of a financial nature

Always be careful when discussing financial matters over email and ensure that the user is who they say they are. It is preferable not to confirm any details with them via this email.



AQUILAI

URL Rewriting

Ajax Intelligence has been given input by the NCSC to ensure it is fully GDPR compliant

- Emails are not stored
- No GDPR defined Personal Information is displayed on publicly accessible user pages
- The ‘To:’, ‘From:’ and ‘Subject’ fields as well as meta data on the Classification results are stored for 30 days
- The only permanently stored data are the ‘To:’, ‘From:’ and timestamp fields
- All data is stored encrypted at rest and in transport in a secure cloud environment
- Access to the stored data is password protected and the secure connection requires separate authorisation

GDPR Compliance

- No company is safe
- Education – Do not rely upon user's alertness
- Automation + AI is a strong extra defense

Peter Horncastle - Meridian RSL
"We find Ajax very effective and easy to setup.
The insurance business has a high level of intermediation with money passing from many entities with a lot of room for error like payment instruction fraud etc"

Phishing affects all organisations – Be prepared

AQUILAI LTD.
Cheltenham

www.aquil.ai