SK ID SOLUTIONS

SK ANNUAL CONFERENCE

4 November 2021

THREAT LANDSCAPE FOR PHISHING & COUNTERMEASURES

Andrew Roberts

What is Phishing

Human Focused

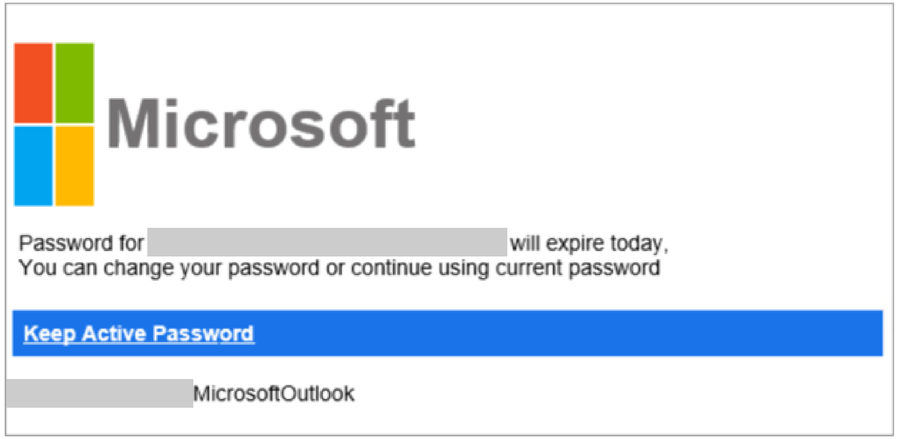
Credential Theft

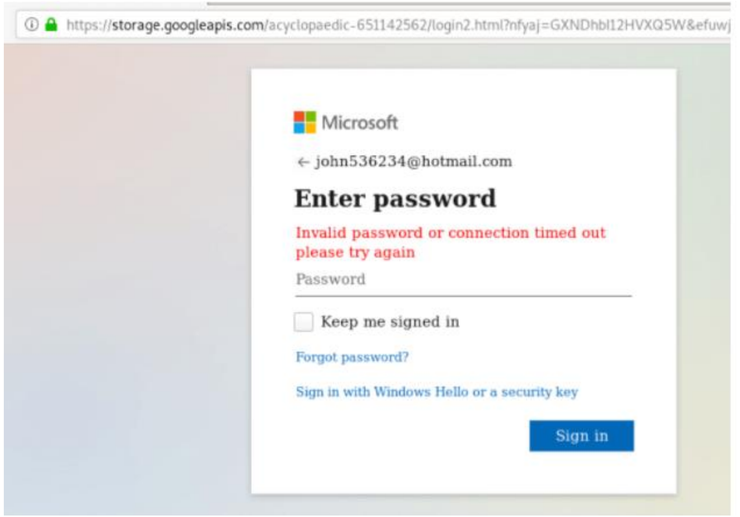
Unauthorized Access

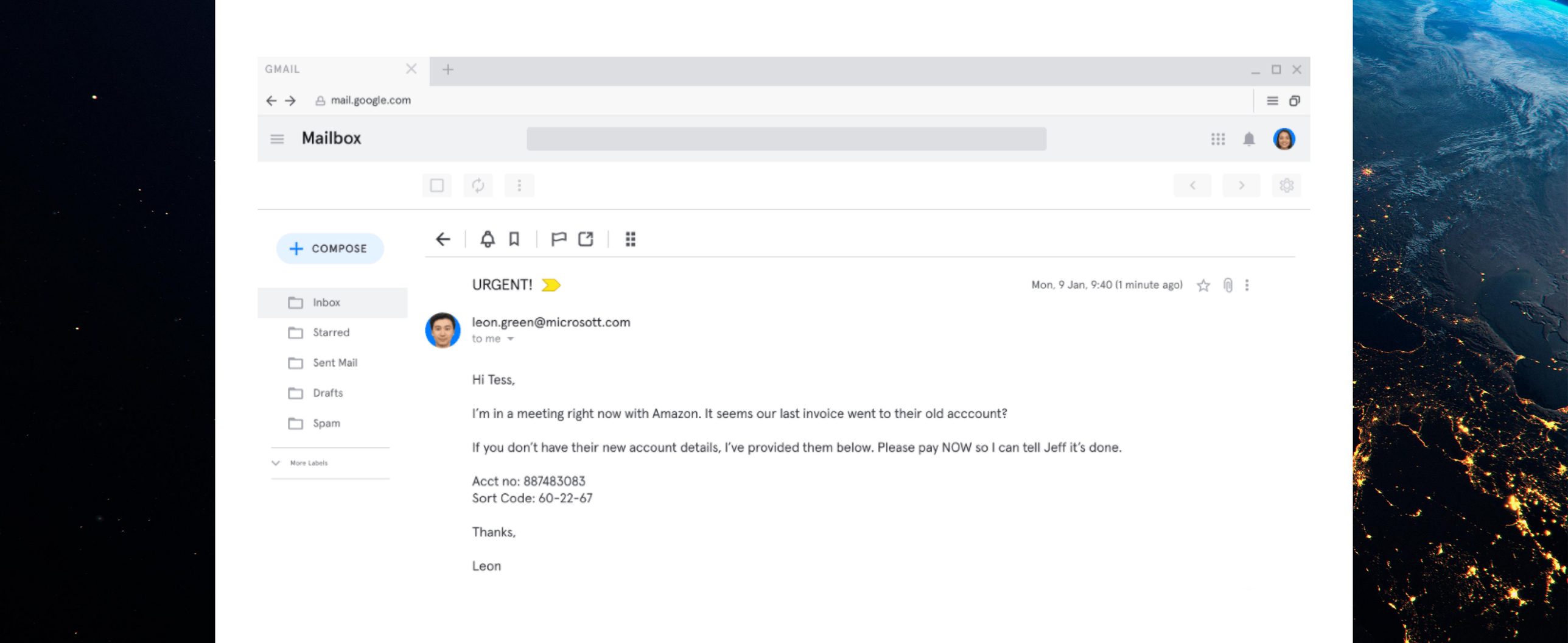
Financially Driven


more give, less take
Help
nab
NAB Internet Banking
NAB ID
Password
Login
Forgotten your NAB ID?
Forgotten your password?
Using NAB Internet Banking for the first time?
Register now
Send money overseas
Save time and money. It's quick and easy online with International Funds Transfers.
Change your daily limit
Need to send a bit more? Change your daily limit easily via NAB Internet Banking.
NAB Defence
NAB invests in the latest fraud prevention technology to ensure you stay safe online.


nab more than money
Wednesday 12 June 2019
Help
Security
Contact us
NAB Internet Banking
NAB ID
Password
Login
Forgotten your NAB ID?
Forgotten your password?
Using NAB Internet Banking for the first time?
Register now
Send money overseas
Save time and money. It's quick and easy online with International Funds Transfers.
Update your details
Moved house? Update your contact details in the Settings menu of NAB Internet Banking.
NAB Defence
NAB invests in the latest fraud prevention technology to ensure you stay safe online.
nabDEFENCE
NAB Defence, your protection against fraud.
Learn more about NAB Defence.

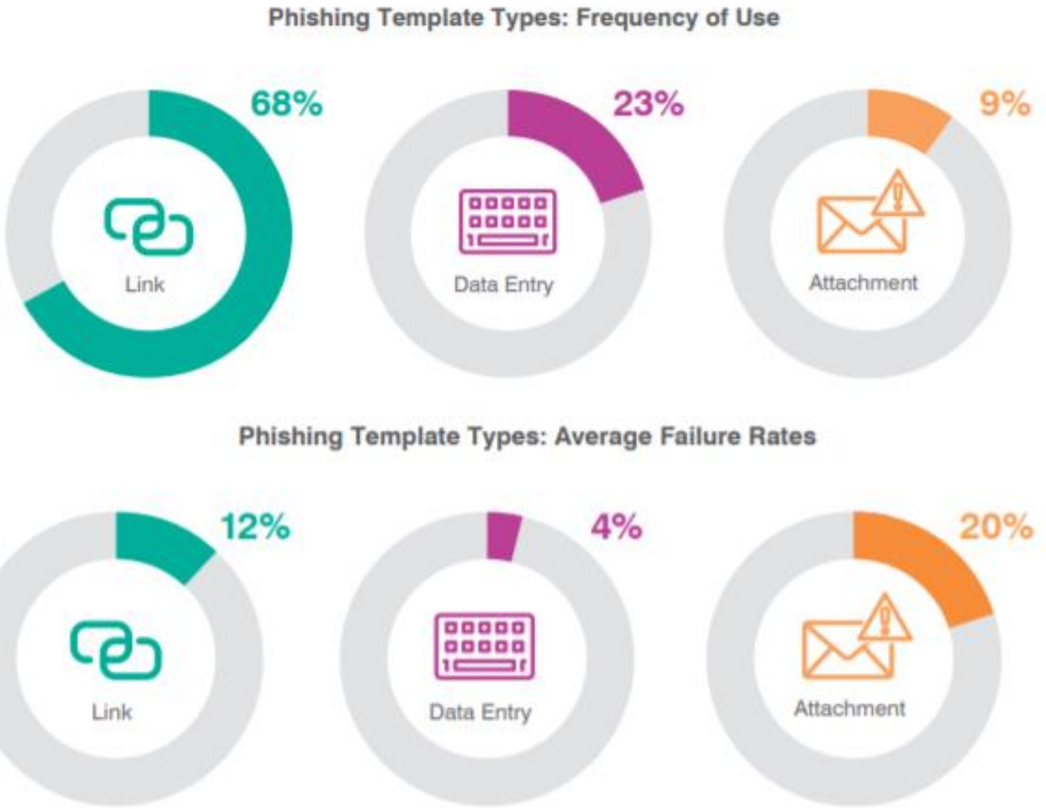

Microsoft
Password for [redacted] will expire today,
You can change your password or continue using current password
Keep Active Password
[redacted] MicrosoftOutlook


https://storage.googleapis.com/acyclopaedic-651142562/login2.html?nfyaj=GXNDhbl12HVXQ5W&efuwj
Microsoft
← john536234@hotmail.com
Enter password
Invalid password or connection timed out
please try again
Password
Keep me signed in
Forgot password?
Sign in with Windows Hello or a security key
Sign in


GMAIL
mail.google.com
Mailbox
COMPOSE
Inbox
Starred
Sent Mail
Drafts
Spam
More Labels
URGENT!
Mon, 9 Jan, 9:40 (1 minute ago)
leon.green@microsott.com
to me
Hi Tess,
I'm in a meeting right now with Amazon. It seems our last invoice went to their old acccount?
If you don't have their new account details, I've provided them below. Please pay NOW so I can tell Jeff it's done.
Acct no: 887483083
Sort Code: 60-22-67
Thanks,
Leon

HUSHPUPPI

Type of Phishing Delivery



Types of Phishing Delivery

- Hidden Text/Zero Font – Evade the Natural Language Processing used to scan for phishing emails
- DNS Hijacking/Redirects – Pharming
- Pop-Ups
- Evil Twin – Rogue Infrastructure: WiFi Hotspot

Global Threat Landscape

ENISA Threat Report 2021

Compromise through phishing e-mails, and brute-forcing on Remote Desktop Services (RDP) remain the two most common ransomware infection vectors.

UK NCSC Weekly Threat Report Oct 2021

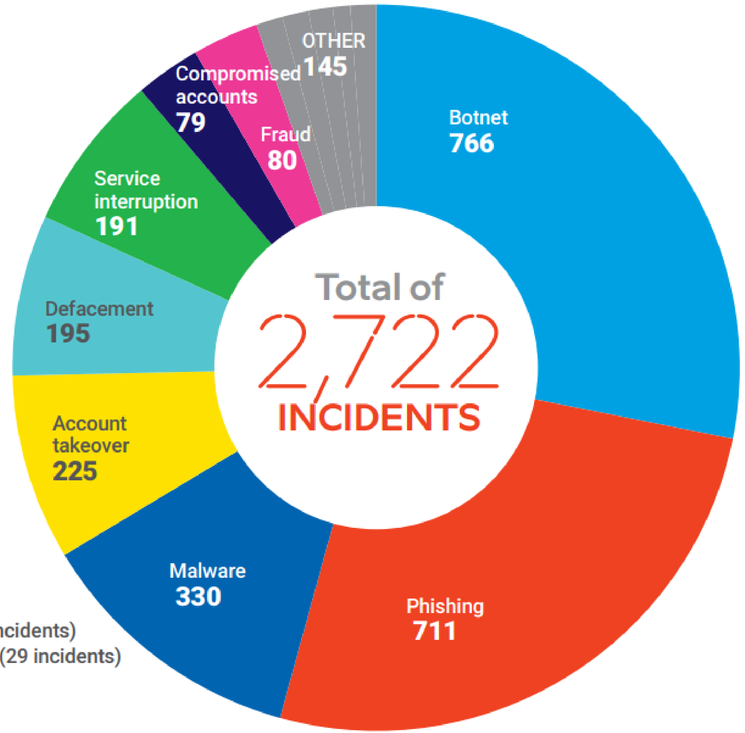
Nearly 45 million people in the UK have been the target of a scam text message or phone call in the past 3 months.

Australia Cyber Threat Report 2021

Phishing campaigns, targeted spear phishing, remote access through vulnerable machines and the use of publicly available exploits remain the most common vectors for deploying ransomware.

Estonian Threat Landscape

Incidents Registered in 2020 which Impacted Data or Systems



'OTHER' includes
- Ransomware (32 incidents)
- Denial-of-service attack (32 incidents)
- Command-and-control server(29 incidents)
- Data leak (21 incidents)
- SEO spam (18 incidents)
- Crypto mining (13 incidents)

Cybersecurity in Estonia 2021 source: https://www.ria.ee/sites/default/files/content-editors/kuberturve/kuberturvalisuse_aastaraamat_2021_eng_final.pdf

2019 – Phishing Campaign targeted at banking and identity services users

2020 – Phishing Campaign using compromised, legitimate accounts

Characteristics of Phishing in Estonia

- Target Users through:
  - Banking Services
  - Small-Business
  - Government Services
- Small Ecosystem
  - Intelligence Gathering is easier for Cybercrime
  - Limited Resources for Defence against Phishing
- Phishing against individuals is targeted at older populace
- Phishing is a continual threat not just a seasonal activity

Trends

- Crimeware-as-a-Service
- New Attack Vectors – Social Media & Personal Devices
- Opportunism - COVID-19
- New Ways of Work – Remote Working
- Digital Transformation – Rich Data Environment

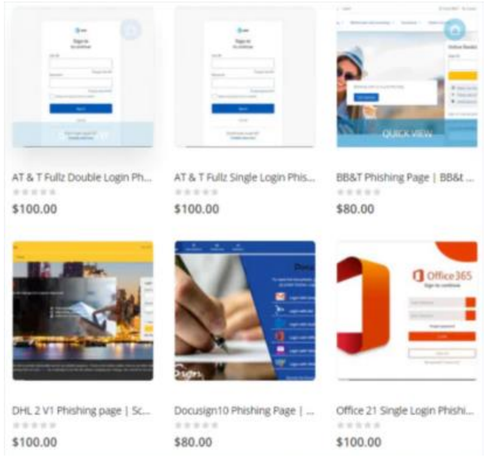
Phishing-as-a-Service

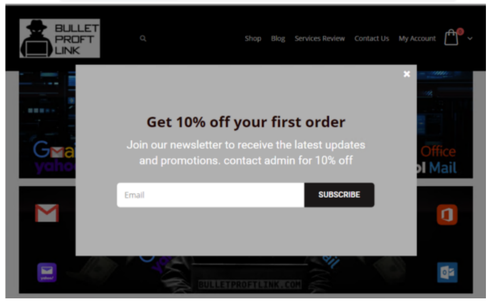
	Phishing kits	Phishing-as-a-Service (PhaaS)
Payment	One-time	Subscription-based *(Available weekly, bi-weekly monthly, or annual)*
Email templates	✓	✓ *(Optional)*
Site templates	✓	✓
Email delivery		✓ *(Optional)*
Site hosting		✓
Credential theft		✓
Credential redistribution		✓
"Fully undetected" links/logs		✓

https://www.microsoft.com/security/blog/2021/09/21/catching-the-big-fish-analyzing-a-large-scale-phishing-as-a-service-operation/

- Phishing Toolkits and Guides readily available
- Phishing often packaged with Ransomware-as-a-Service

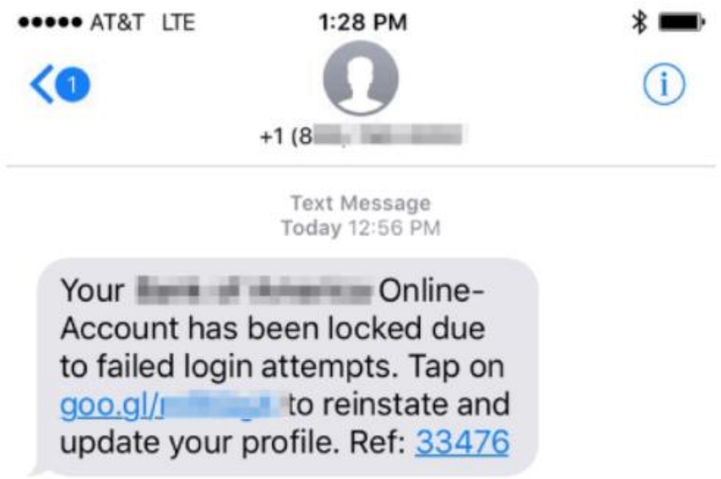
Phishing-as-a-Service





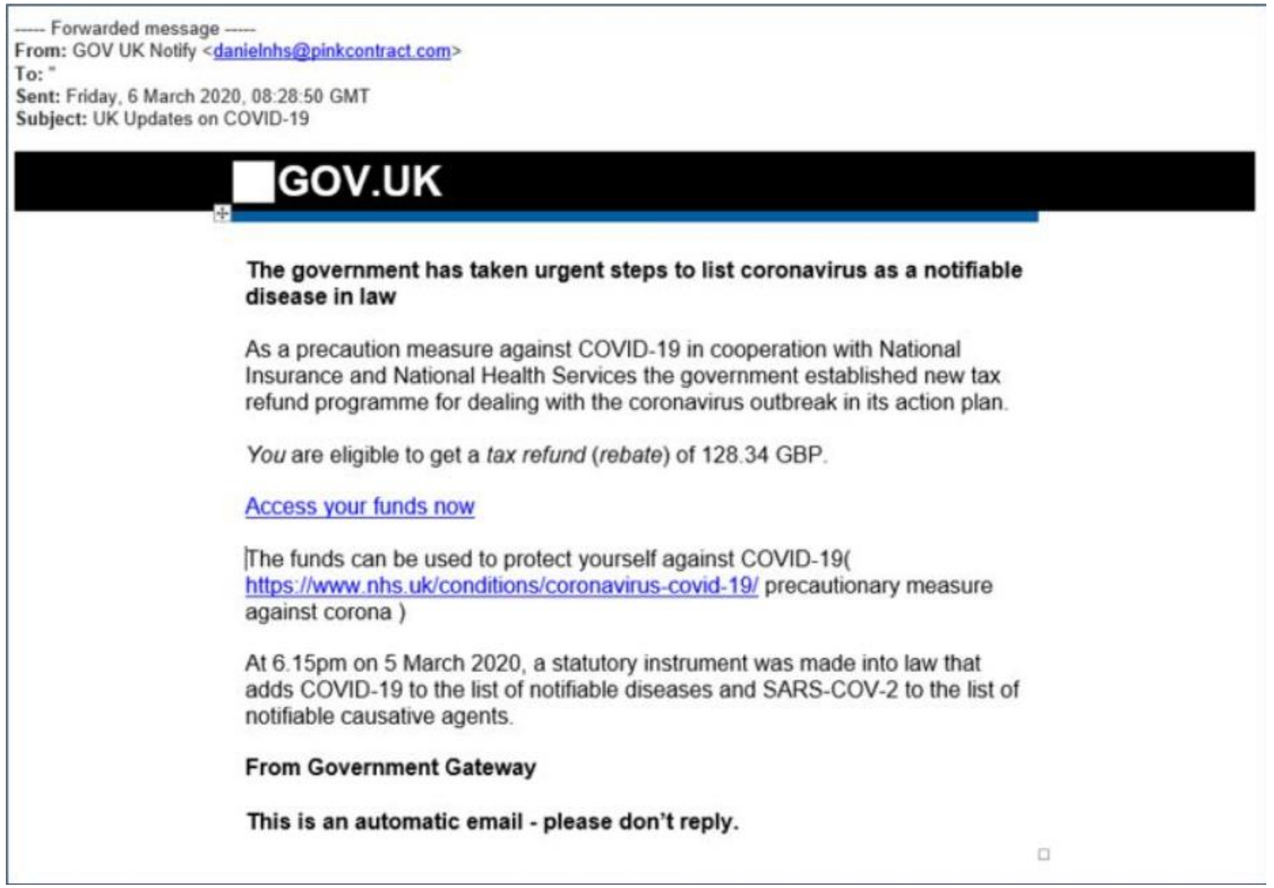
- BulletProof Link commercial phishing company
- Provided commercial phishing services and YouTube how-to guides on phishing
- 100 Available phishing templates of known brands and services
- Host infrastructure of the Phishing Company was identified but attribution not possible

New Attack Surfaces



- Gaming Accounts
- Social Media
- Mobile - SMS

COVID-19



----- Forwarded message -----
From: GOV UK Notify <danielnhs@pinkcontract.com>
To: "
Sent: Friday, 6 March 2020, 08:28:50 GMT
Subject: UK Updates on COVID-19

GOV.UK

The government has taken urgent steps to list coronavirus as a notifiable disease in law

As a precaution measure against COVID-19 in cooperation with National Insurance and National Health Services the government established new tax refund programme for dealing with the coronavirus outbreak in its action plan.

You are eligible to get a *tax refund* (*rebate*) of 128.34 GBP.

Access your funds now

The funds can be used to protect yourself against COVID-19(https://www.nhs.uk/conditions/coronavirus-covid-19/ precautionary measure against corona)

At 6.15pm on 5 March 2020, a statutory instrument was made into law that adds COVID-19 to the list of notifiable diseases and SARS-COV-2 to the list of notifiable causative agents.

From Government Gateway

This is an automatic email - please don't reply.

COVID-19

Saatja: Terviseamet [mailto:finansije@hotel-n.rs]
Saatmisaeg: 21. august 2020 10:32
Teema: Covid-19 kaitsevahendite tasuta levitamine (Eesti Vabariik Terviseamet)
Tähtsus: Kõrge

Eesti Vabariik
Terviseamet

Lugupeetud kodanikud

Vastavalt 25-2-2020 seadusandliku siseseaduse (Valitsuse Eesti 42 / A / 25-2-2020) artiklile 3 "Kiireloomulised meetmed koroonaviiruse leviku tõkestamiseks ja piiramiseks".

Meie, Eesti Tervishoiuministeerium, levitame koostöös Eesti valitsusega covid-19 näomaski, respiraatoreid, testimismasinaid ja muid kaitsevahendeid covid-19 tasuta kõigile Eesti registreeritud ettevõtetele, mida koordineerib terviseregioonide kesknõukogu (TK). Täitke lisatud vorm ja veenduge, et sellele vormile on kirjutatud täpne töötajate arv ja ettevõtte aadress.

Täitke lisatud vorm ja saatke meile koopia enne sulgemist täna ja ootame teie kiiret vastust.

Saatke kõik täidetud vormid sellele e-posti aadressile: covid-19@terviseamet.ee

Tervitused

Riina Sikkut
Tervise- ja tööminister

Eesti Vabariik
Terviseamet

Terviseamet
Paldiski mnt 81, 10617 Tallinn
Telephone: (+372) 794 3500
covid-19@terviseamet.ee
https://www.terviseamet.ee/

New Work Environment

- Working from Home & Virtualisation of the workforce
- Psychologically breaks the link between the work environment and home environment
- Many companies not adapted to provide remote working technical facilities

Rich Data Environment

U.S. LEGAL NEWS DECEMBER 1, 2018 / 2:55 AM / UPDATED 3 YEARS AGO

Marriott's Starwood database hacked, 500 million may be affected

By Jim Finkle, Arjun Panchadar

3 MIN READ

(Reuters) - Marriott International said on Friday hackers stole about 500 million records from its Starwood Hotels reservation system in an attack that began four years ago, exposing personal data of customers including some payment card numbers.

Rich Data Environment

Free Identity Monitoring

Where available in your country/region, Marriott is offering affected guests the opportunity to enroll in a personal information monitoring service free of charge for one year. This will be provided by Experian, a global data and information service provider. This service (IdentityWorks℠ Global Internet Surveillance) is available to residents of Australia, Brazil, Germany, Hong Kong, India, Ireland, Italy, Mexico, New Zealand, Poland, Singapore, Spain and the Netherlands. (Experian does not currently offer this service in all countries or regions.)

IdentityWorks℠ Global Internet Surveillance monitors whether your personal data is available on public websites, chat rooms, blogs, and non-public places on the internet where data can be compromised, such as "dark web" sites, and generates an alert to you if evidence of your personal information is found.

Rich Data Environment

Please visit the following website: https://www.globalidworks.com/identity1 and click the "Get Started" button to activate this 12-month complimentary service. You can then enter the activation code: K9QX65ZN3TR3 to start your IdentityWorks℠ Global Internet Surveillance membership.

The section below provides additional information on steps you can take. If you are a resident of the United States, UK, or Canada, please check info.starwoodhotels.com for similar services being offered in those countries.

Rich Data Environment

Hack Brief: Marriott Got Hacked. Yes, Again

The hotel chain has suffered its second major breach in 16 months. Here's how to find out if you're affected.

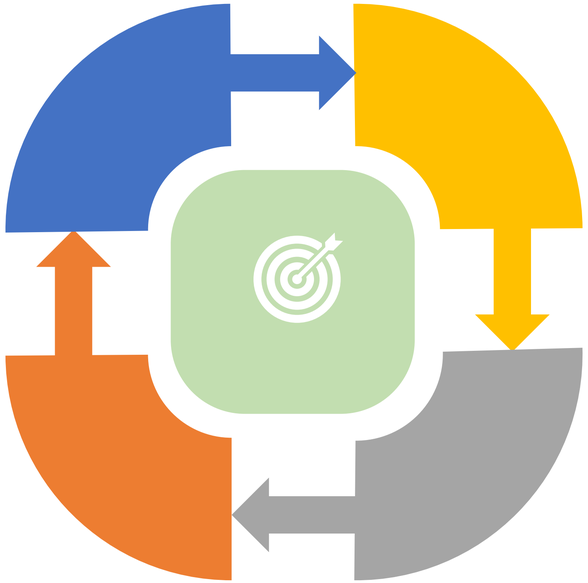
Countermeasures

Damage Mitigation

- Contain any financial and data loss
- Incident Response plans tailored for phishing
- Information Sharing

User-Awareness

- Train Users to detect and respond to malicious phishing content
- Awareness of those offering services that are targets of phishing



Detection/Prevention

- Personal Device Security
- Block Untrusted Sources
- Patched System, Mail Filtering, Anti-Virus, Multi-Factor Authentication

Monitoring

- Telecommunication Providers can block known phishing sources
- Network monitoring

Four Layer of Phishing Defence

The Human Firewall

User Awareness Training

- Phishing Simulation Exercises
- Builds awareness of the User to signs of a malicious email source

Evil Phishing Tests

- Presents extreme phishing simulations that test the ethical boundaries of organisations experiments.

Passwords

- HaveIbeenPwnd
- Multi-Factor Authentication

Incident Response

- Incident Response Plans for Phishing should be exercised regularly through table-tops and phishing simulation exercises

- Information sharing between related organisations is of vital importance but there are impediments to what data can be shared with who

- The Phishing Kill-Chain or Cybercrime Journey needs to be mapped to understand the adversarial perspective and derive key weaknesses

Conclusion

- Phishing will remain one of the top cyber threats due to its low cost of implementation and high effectiveness.
- Defence mechanisms need to include solutions for people, process and technology.
- Information sharing and exercises/simulations should be a core part of defence of phishing