Phishing Trends
ISITPHISHING.AI

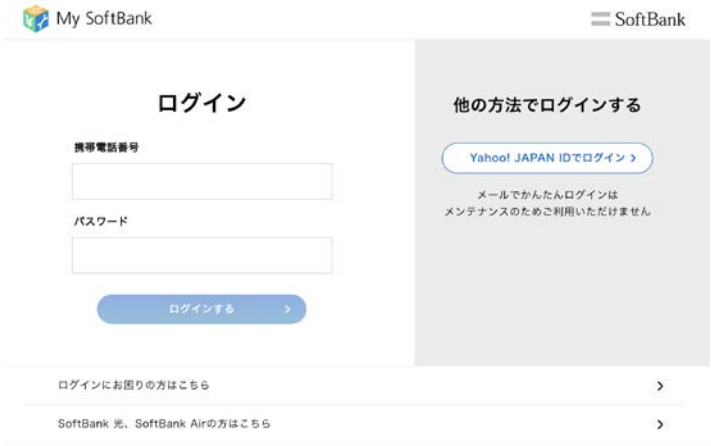
JPAAWG, Tokyo, November 8th 2018

Olivier LEMARIE

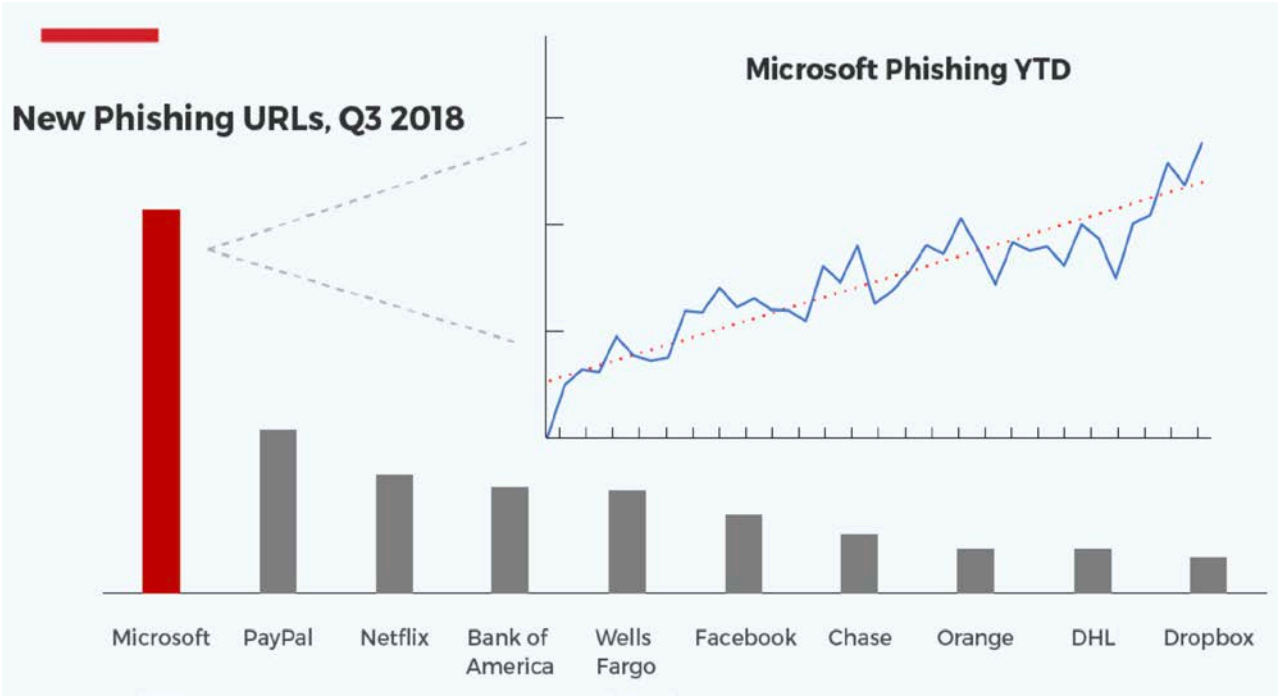
CTO

Phishing Trends Overview

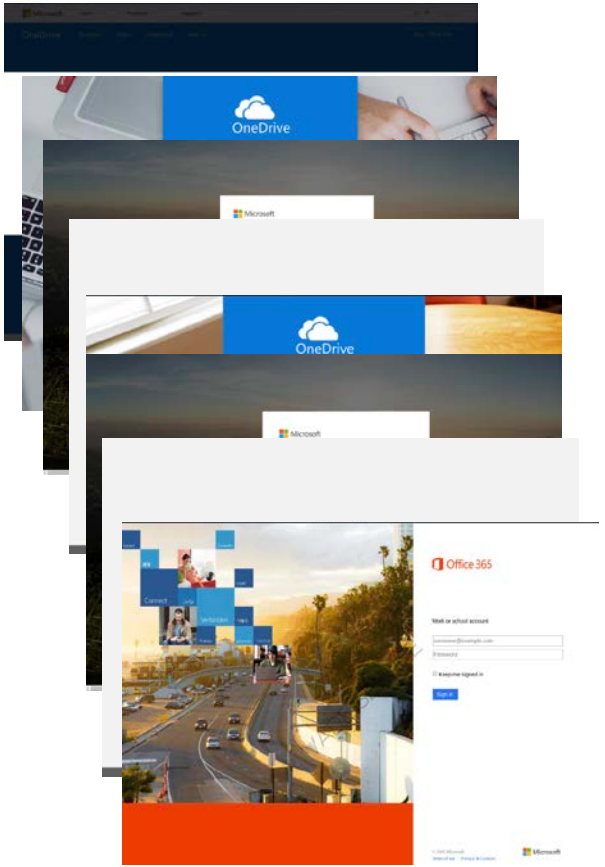
- Rise of credential phishing attacks
  - Gaining access to a treasure trove of confidential files, financial data, contacts,..
- Compromised accounts to fuel additional attacks
  - Sending Emails but also to conduct spear phishing, or other insider attacks
- High level of sophistication
  - Defeating traditional layers of protection
- Industrialization of Phishing
  - With significant financial capacity



Trend : Phishing Targeting Businesses

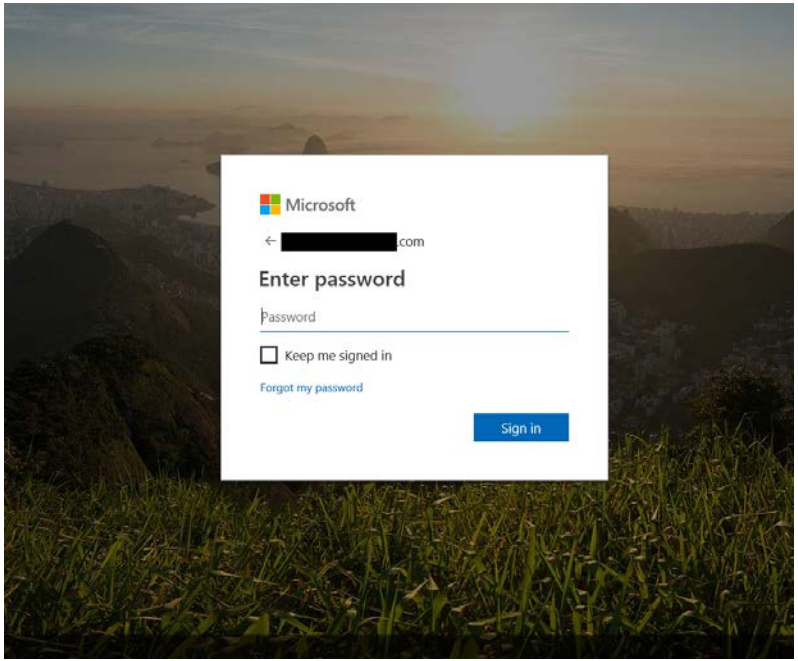


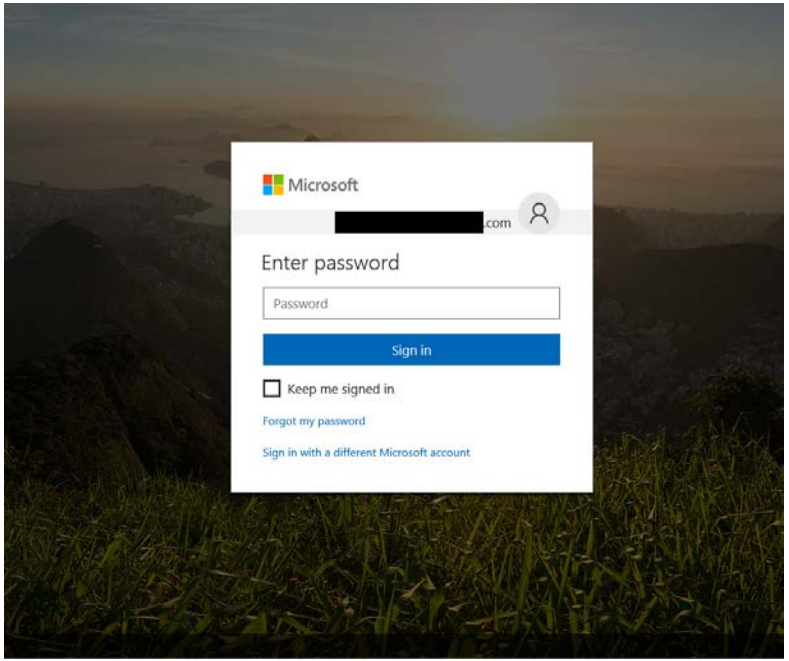
Source : Vade Secure Phisher's Favorites Report Q3 2018



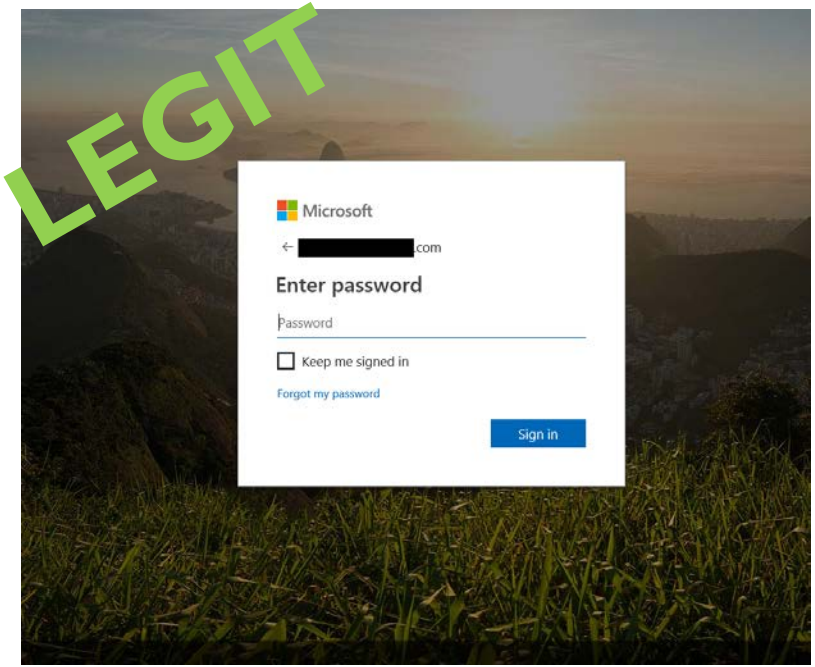
Source : IsItPhishing.AI

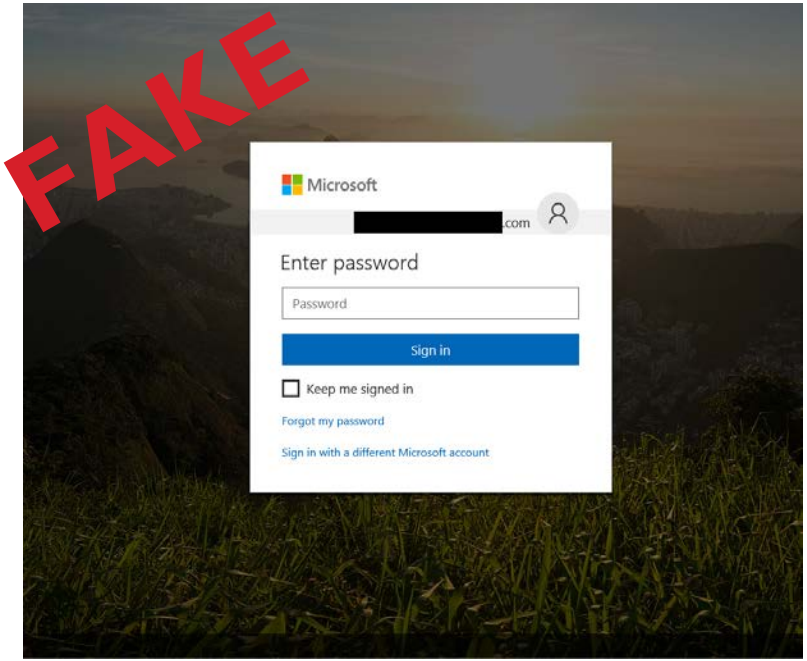
Can you “still” spot the real Office 365 login page ?





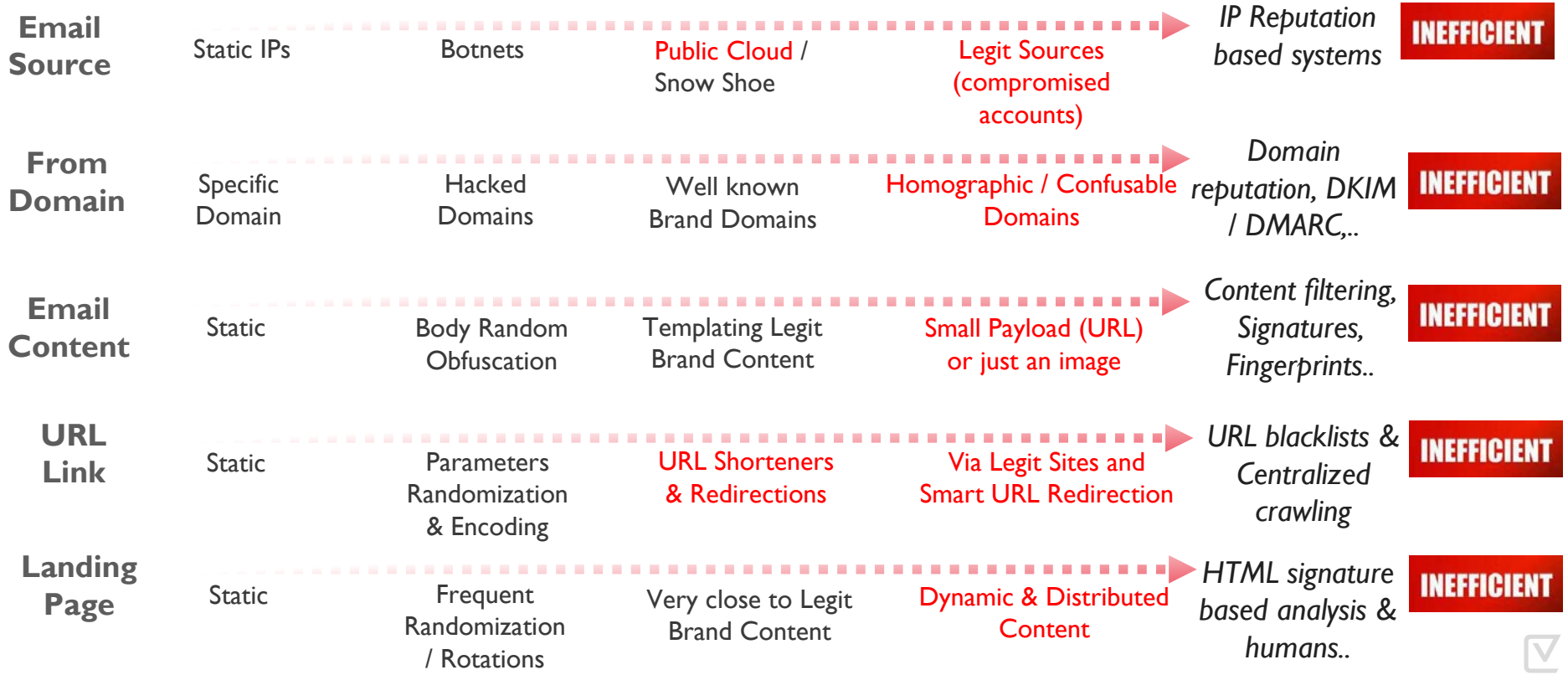
Can you “still” spot the real Office 365 login page ?



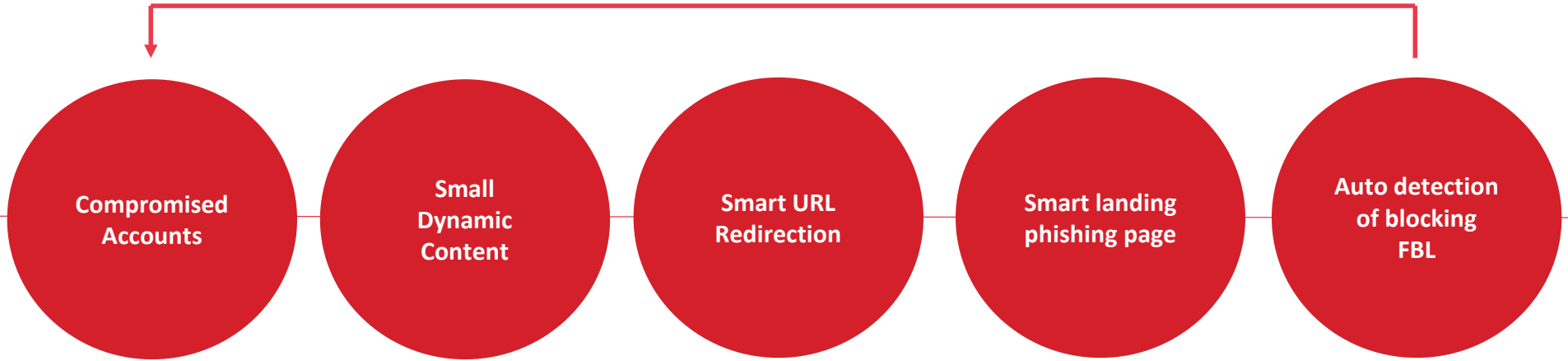


Trend: Higher Content Quality to Drive Phishing Effectiveness

Trend : Combining Technics to Defeat Traditional Layers of Protection



Example: Targeted credential phishing attack (Oct 2018)



- Targeting one large ISP
- More than 150,000 compromised accounts
- 10 minutes cycles
- Below threshold volumes

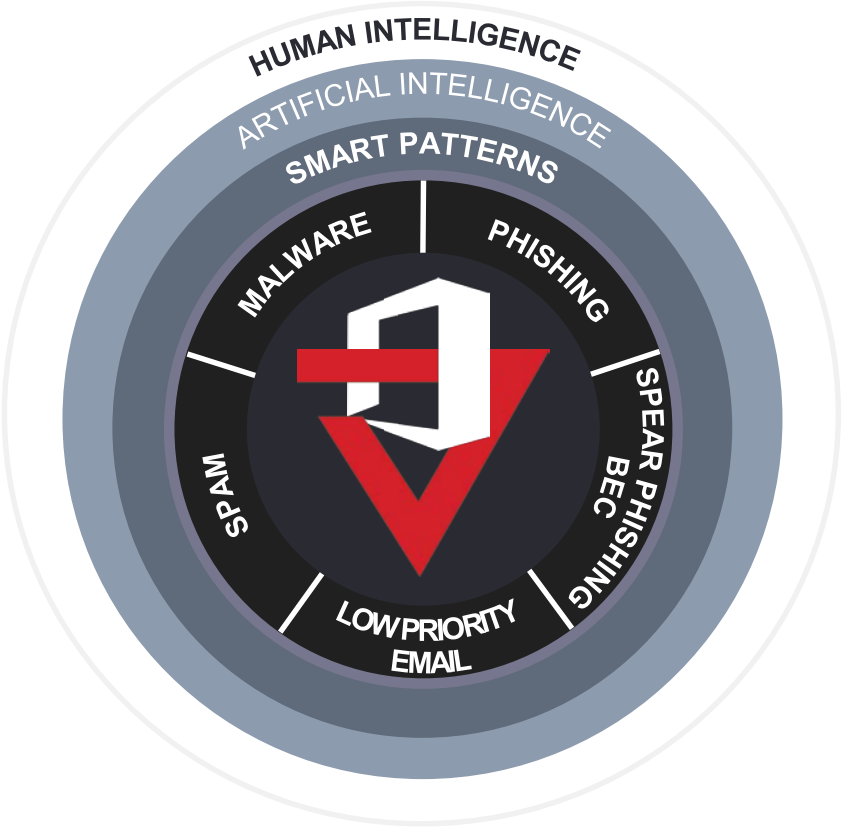
- Every email different in structure and payload
- Several legit urls
- 1 phishing URL (never the same)

- Variety of redirection technics (shorteners, tracking..)
- Rotation out of 25,000 domains specifically registered for the attack (2 months before)

- Serving content only for few minutes
- And not at time of email delivery

- Thousands of canary accounts
- Instant detection of blocking and rotation

AI To Address New Challenges



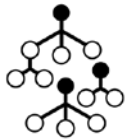
- Not replacing but complementing existing filtering layers
- Allowing the detection to happen from the first email
- Processing massive amount of data in realtime
- Expertise driven approach
- Prediction Models build out of features extracted from source, content & context of the emails.
- Moving towards predictive models

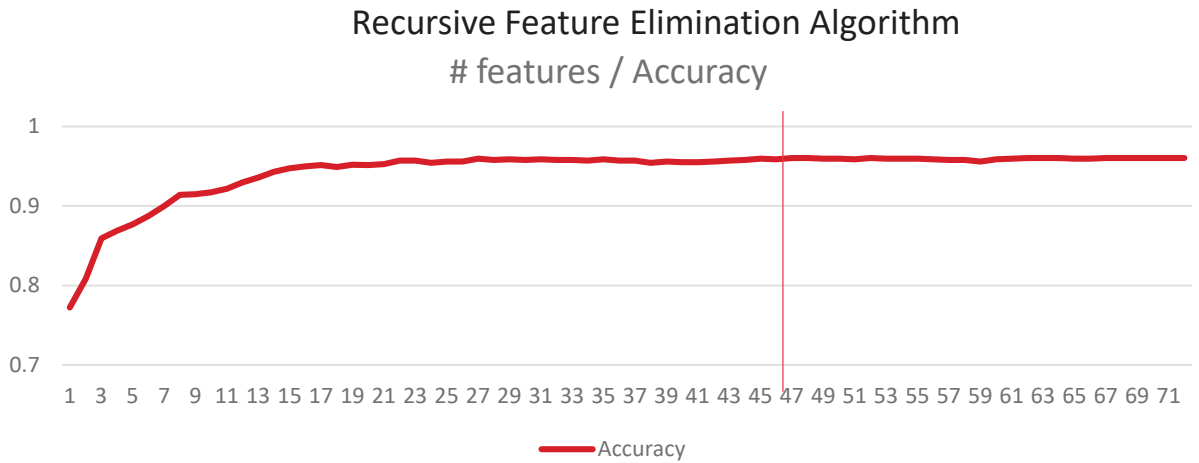
Machine Learning Predictive Models for Phishing

- Models for Phishing detection integrated in our IsItPhishing.AI platform
- Analysis of urls and documents in real time at time of click
- Selected 47 features to drive for effectiveness

Support Vector Machine

Random Forest





- 2 others areas of focus in roadmap :
  - Computer Vision / Phishing Brand detection
  - Targeted Attacks Detection

Machine Learning Models for Spear Phishing

Example: CEO Fraud / Business Email Compromise(BEC)

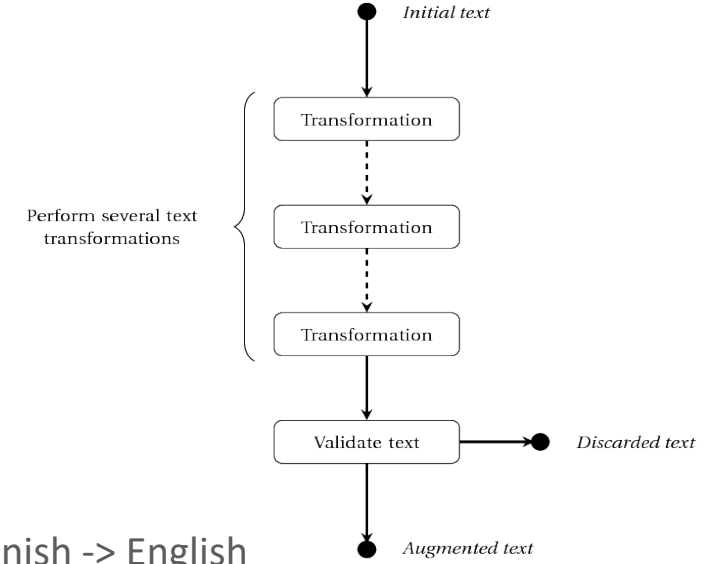
> *I need you to arrange a transfer of $140,000 to a supplier today. It is for an acquisition that we have been trading privately for a few weeks and the supplier has accepted our payment terms of 10 % down payment. Let me know if you can do it immediately, I can send you the bank details.*

- Highly damaging
- Using Employee impersonation
- Extremely rare
- Often text based only

- Anomaly detection FP rate can be high
- Natural Language Processing (NLP) requires a lot of tuning
- Classification / Machine Learning requires quantitative and qualitative data

Data Augmentation Technics

- Presented at MAAWG NYC last month
- Enrich a dataset used to construct models
  - Synonyms Replacement, Mispelling, Name Replacement, Amount transformation, Language Translation,..
- Ensure quality of augmented data
  - Semantic similarity, Syntactic similarity



Example on CEO Fraud : English -> French -> Spanish -> English

```
Hi,
I need you to arrange a transfer of $140,000
to a supplier today. It is for an acquisition
that we have been trading privately for a few
weeks and the supplier has accepted our
payment terms of 10 % down payment. Let me
know if you can do it immediately, I can send
you the bank details.
Thank you.
Sincerely
Sandy
```

```
Hello, I'll need you to arrange a transfer
of 136,700 € to a vendor today. This is
for an acquisition that we have been
negotiating privately for some weeks and
the vendor agreed to our payment terms of
10% down payment. Let me know if you can
get this done immediately, I can forward
you the bank details.
Thanks.
Best regards
Irene
```

Vade Secure
Predictive Email Defense

Thank You