Everything and Nothing

Aamir Lakhani (A^2
Senior Red Team Researcher

Aamir Lakhani

Global Security Strategist/Researcher

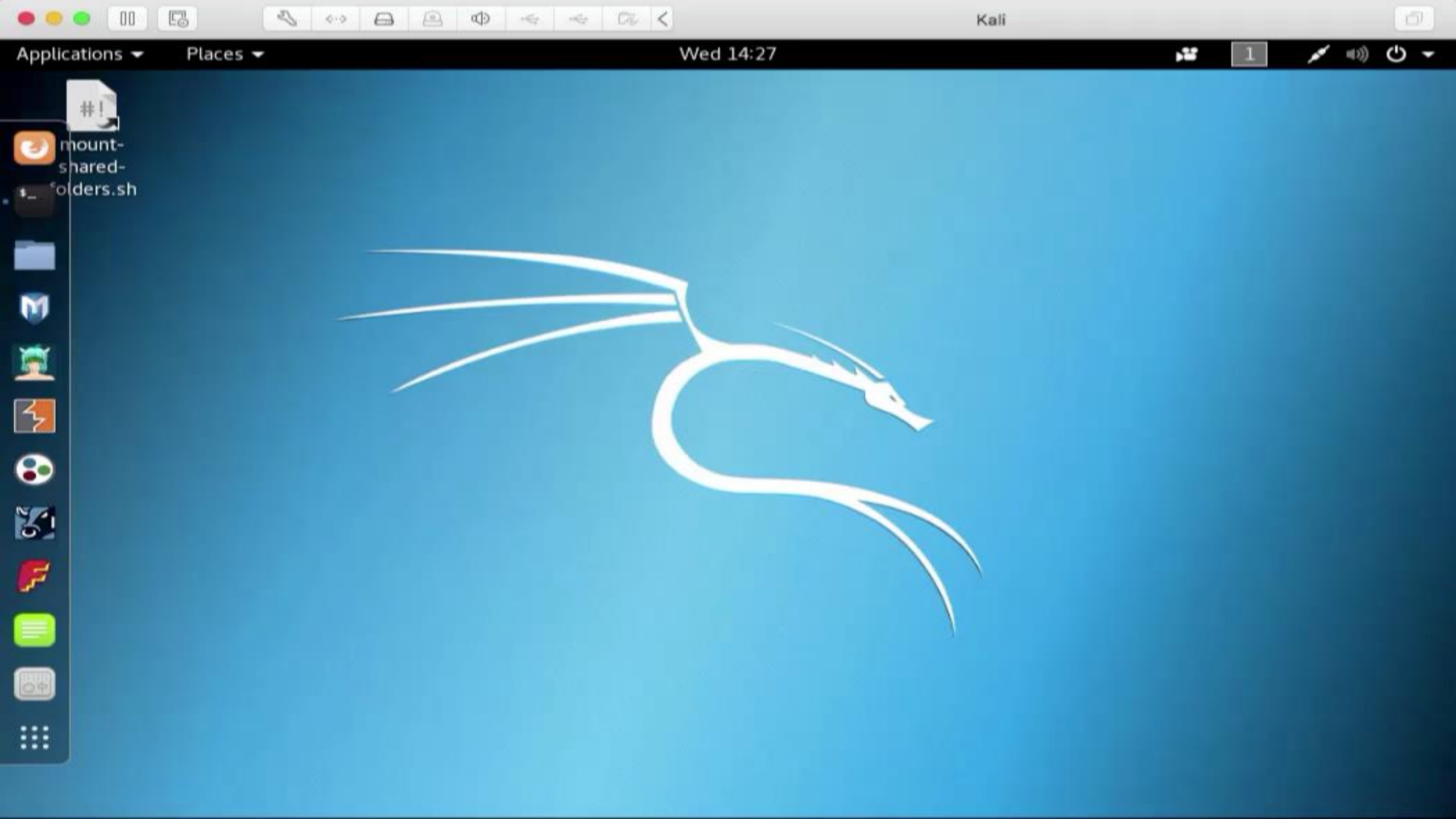
HACKER, GAMER, NINJA

- 20+ years in IT and Security Industry
- Offensive Security Specialist
- Cybercrime Investigator
- Lead Threat Intelligence researcher
- Author of books, training certifications, cyber courses
- **aamir.lakhani@me.com**

IS HACKING EASY

WHO ARE THE HAKERS

IS HACKING CONSIDERED GOOD


Kali
Applications
Places
Wed 14:27
1
mount-shared-folders.sh

Most Hackers Are NOT Attackers

Most Hackers Are NOT Cyber Criminals

- **Knowing**
  Someone can Remotely Stop a Pacemaker
- **Finding**
  Hidden violations of privacy in smartphone
- **Getting**
  Unlimited lives in a video game

Attackers

Illegally Profit from Cyber-Crimes

Destroy, Manipulate, or Abuse Technology

Describe themselves as **Hackers**

Cloud and Corporate Attacks

- FortiGuard Labs has seen a 300% increase in RDP attacks since 2019
- VPN Hijacking attacks occur when improper VPN configurations are implemented
  - Implement 2-Factor Authentication
  - Don’t configure Split Tunneling
  - If possible, use client checks such as certificates or NAC policies.
- Increase in shadow IT projects, public VNC and other remote systems
- Rapid deployment of cloud and web applications

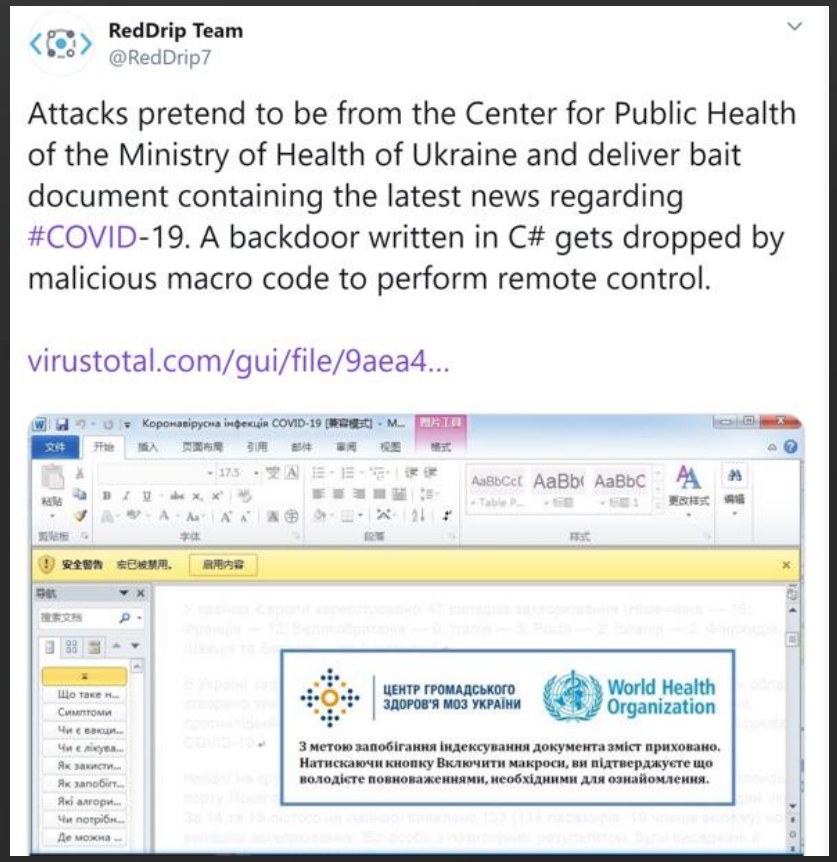
Phishing

Phishing Websites detected by Google (2020)

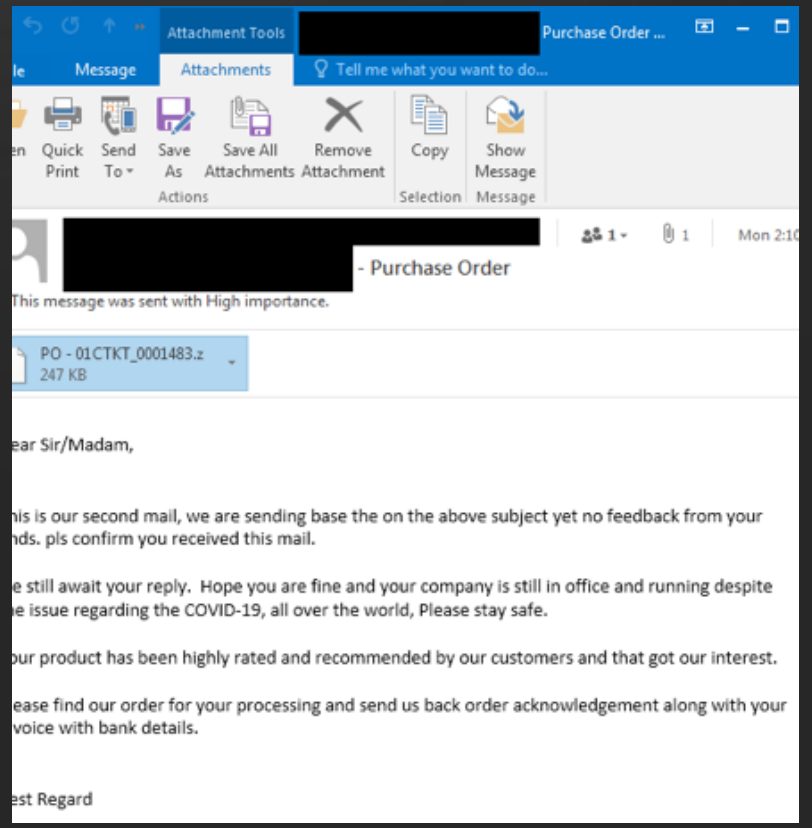
350% increase since January

Phishing attacks are on the rise

Banking and Financial



Macro with malicious functions such as RATs and other access trojans



Emails with Attachments

Ransomware Attacks

covid19fund@smmesa.gov.za | info@wsk.co.za | 1 | Wed 5/1

COVID-19 Relief Payment Approval (Ref: C19V202991)

We removed extra line breaks from this message.

COVID-19 Relief Paym...
0 bytes

Ref: C19V202991

Dear Beneficiary,

As part of the Government Financial Aid Programme, you have been approved to receive COVID-19 Relief Payment from June - August 2020 through the Temporary Employer/Employee Relief Scheme (TERS).

You are required to complete the attached Payment and Acceptance Forms 1B and 3A, and return to us by email or fax using the details and reference number provided on the form.

Regards,

TERS Covid-19 Administration Team
Compensation House
167 Thabo Sehume Street, Delta Heights Building Pretoria
Phone:0800 030 007

THE WORLD BANK
IBRD • IDA

THE WORLD'S BANK Washington, D.C., United States

International Banking

FOREIGN EXCHANGE UNIT

THE TELEX AND CREDIT SECTION, FUND MONITORING AND AUTHORIZATION OFFICE

RE CONFIRMATION OF WORLD BANK-HSBC BANK RELIEF PAYMENT FUND

Attention: Beneficiary.

This is to notify you that after series of meeting with our board of directors held in the United States ,the World Bank-HSBC Bank has mandate to set aside a Covid-19 Compensation Relief Funds due to the current Pandemic to assist the Business-Personal, mostly to boost the business package, the countries due on this package are Asia, ,America,Europe,Africa,worldwide, we have decided to use this hard time of COVID-19 Pandemic to carry on the release of the fund by ourselves as approved on 18th of March 2020 when we asked our affiliate bank (Barclays and Bank of America) regarding the release of the Compensation Business Relief Funds to the beneficiaries who's email address materialize on our database. The World bank President (Mr David R Malpass) has given the Inland Revenue Services Department of England go ahead to work with HSBC Bank London ,This Instruction was made after (The HSBC Bank) was charged of $1.92 Billion to Settle Charges of Money Laundering and was carry on this period as published in this site

(https://dealbook.nytimes.com/2012/12/11/hsbc-to-pay-record-fine-to-settle-money-laundering-charges/)

Because of this, the WORLD BANK-HSBC Bank London has chosen a capable affiliate Bank of our choice to handle the Compensation Covid-19 Relief Funds with Barclays Bank. Therefore, you are to contact the compensation Broker bellow: Mr Ben Middleton on how to receive your Compensation Relief payment with our assigned Accountant paying officer from Barclays Bank London However, We apologize for the delay of your payment and all the inconveniences that we might have caused you during this period. The Sum of $850,000.00 (Eight Hundred and Fifty Thousand United States Dollars) will be pay to you through Loaded Unlimited international ATM MASTER or ATM VISA Card and post to your address. Noted your compensation amount been insured to avoid mishandle or double payment.

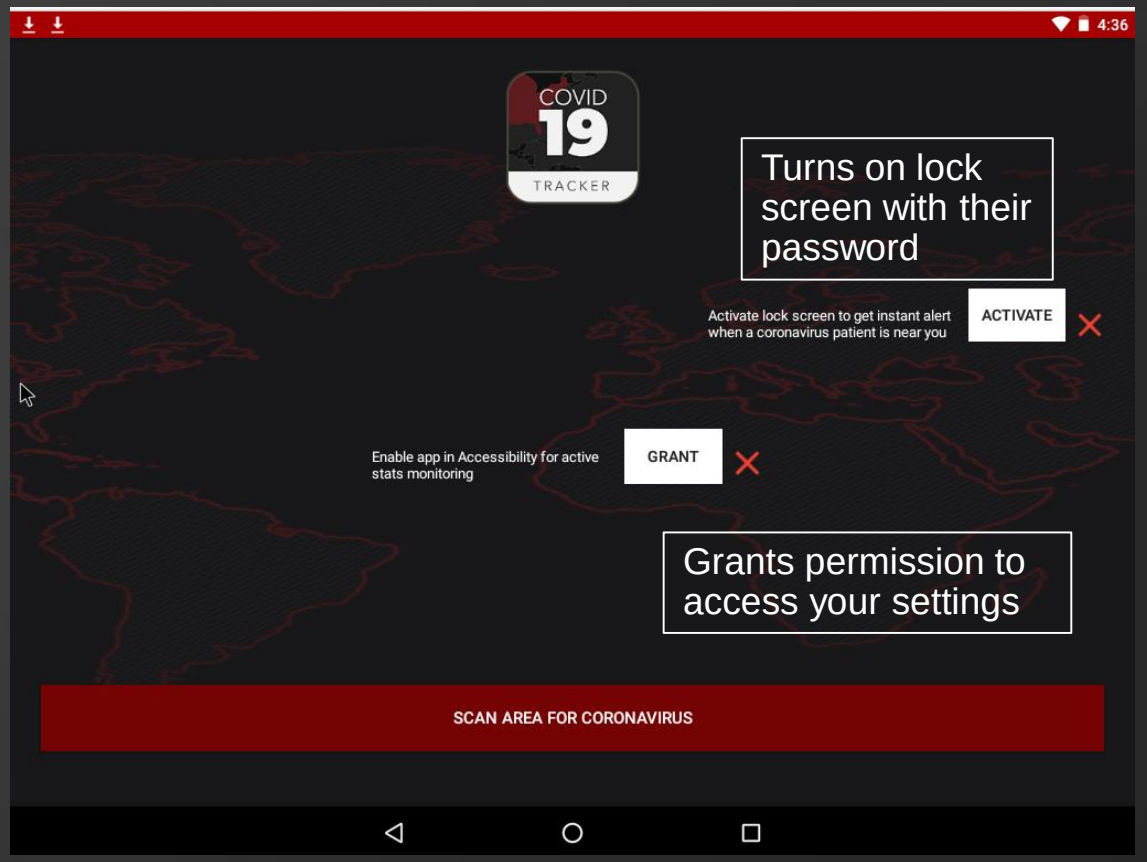
Your Full Names_____You're Address_____

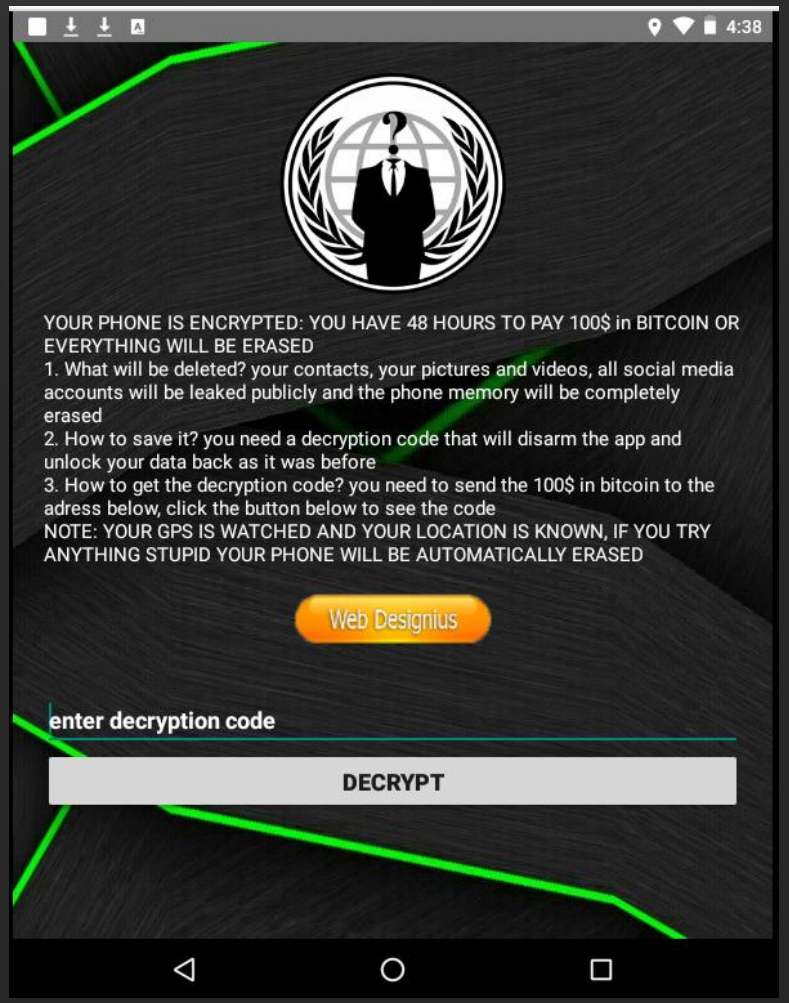
Phone Number_____ Your Age_____ Occupation_____

Therefore, you are to contact on this email with the below details to direct you on how to receive your fund through our compensation broker : E-mail benmiddleton2@email.com/benmiddleton2@writeme.com or call him: line: +447441392060, Please Be Warned, as The world Bank does not instruct any other Bank or agent in this payment except (Mr Ben Middleton), whom we can only give attention to, and from now,

Best Wishes

The World bank President (Mr David R Malpass


4:36
COVID 19 TRACKER
Turns on lock screen with their password
Activate lock screen to get instant alert when a coronavirus patient is near you
ACTIVATE
Enable app in Accessibility for active stats monitoring
GRANT
Grants permission to access your settings
SCAN AREA FOR CORONAVIRUS


4:38
YOUR PHONE IS ENCRYPTED: YOU HAVE 48 HOURS TO PAY 100$ in BITCOIN OR EVERYTHING WILL BE ERASED
1. What will be deleted? your contacts, your pictures and videos, all social media accounts will be leaked publicly and the phone memory will be completely erased
2. How to save it? you need a decryption code that will disarm the app and unlock your data back as it was before
3. How to get the decryption code? you need to send the 100$ in bitcoin to the adress below, click the button below to see the code
NOTE: YOUR GPS IS WATCHED AND YOUR LOCATION IS KNOWN, IF YOU TRY ANYTHING STUPID YOUR PHONE WILL BE AUTOMATICALLY ERASED
Web Designius
enter decryption code
DECRYPT


Internet of Very Bad Things

Skill Squatting – How It Works

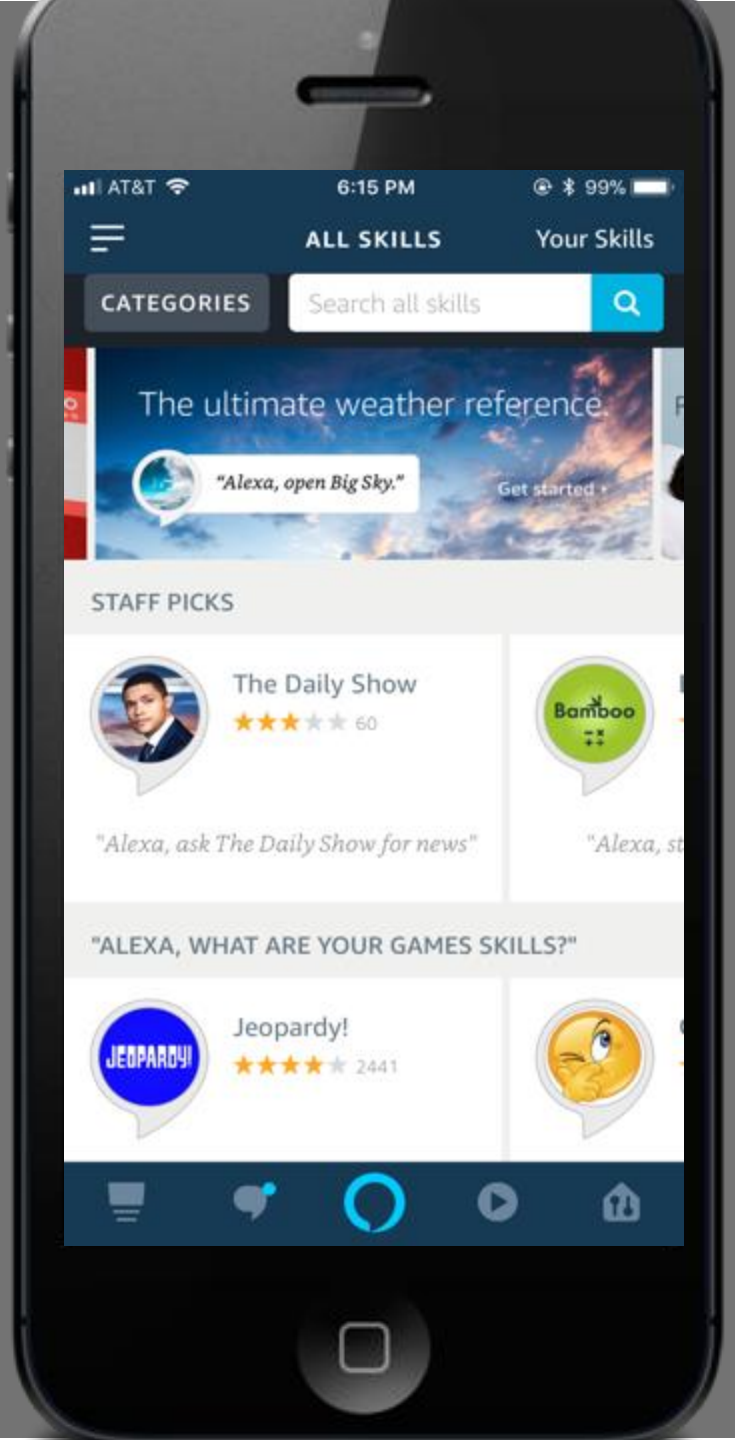
Criminals

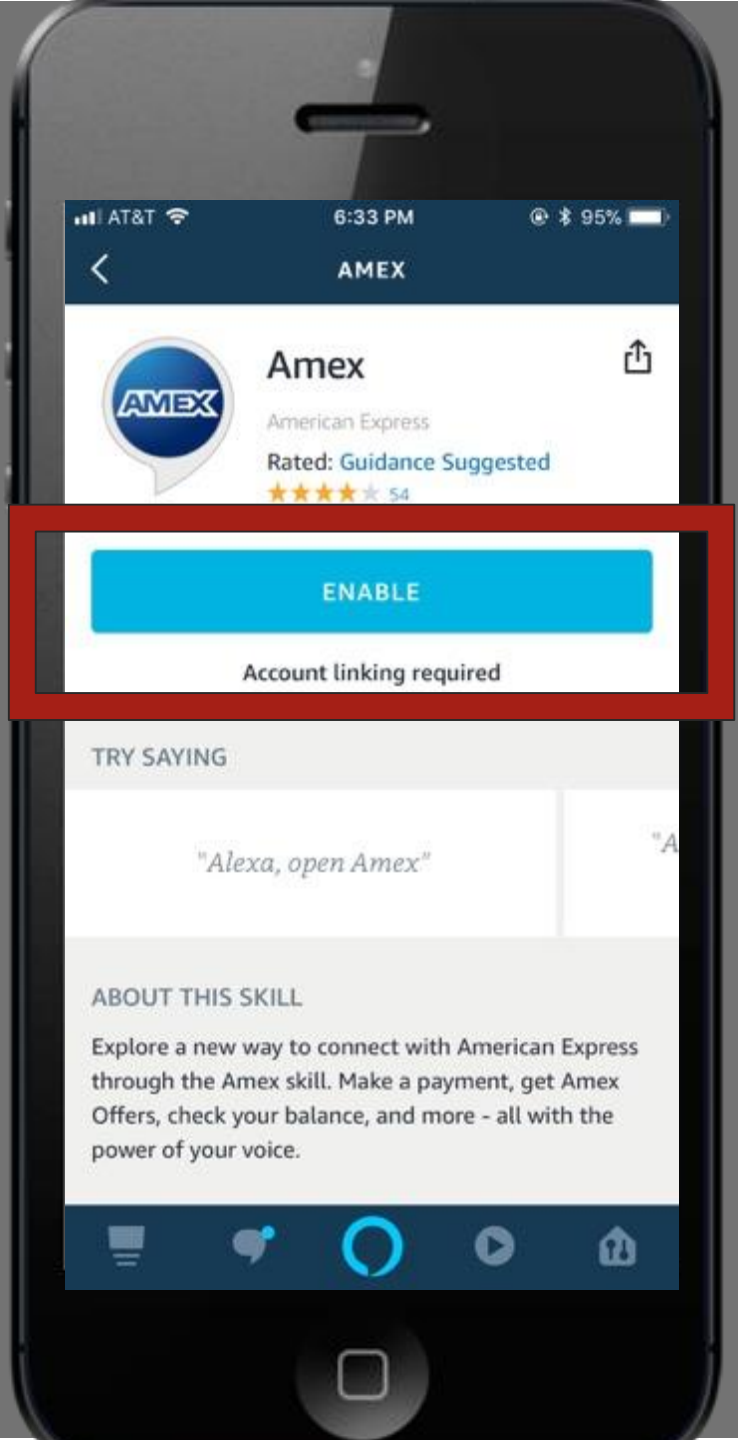
Sound-alike Skill "Name"

Publish Skill

User enables "Skill"

Alexa, open "Skill Name"


AT&T
6:15 PM
99%
ALL SKILLS
Your Skills
CATEGORIES
Search all skills
The ultimate weather reference.
"Alexa, open Big Sky."
Get started ›
STAFF PICKS
The Daily Show
60
"Alexa, ask The Daily Show for news"
Bamboo
"ALEXA, WHAT ARE YOUR GAMES SKILLS?"
Jeopardy!
2441


AT&T
6:33 PM
95%
AMEX
Amex
American Express
Rated: Guidance Suggested
54
ENABLE
Account linking required
TRY SAYING
"Alexa, open Amex"
ABOUT THIS SKILL
Explore a new way to connect with American Express through the Amex skill. Make a payment, get Amex Offers, check your balance, and more - all with the power of your voice.


02:03 PM
Trash
File System
Home


Home | Houston | Dr. Chaos
https://www.drchaos.com
Dr. Chaos
Dark Security and Total Chaos Blog
HOME
CONTACT US
MEDIA LINKS
AAMIR LAKHANI
DISCUSSIONS, CONCEPTS & TECHNOLOGIES FOR THE WORLD OF
CYBER & INFOSEC
"blogger, InfoSec specialist, super hero ... and all round good guy"
JOIN THE DISCUSSION

```
[*] WE GOT A HIT! Printing the output:
PARAM: GALX=SJLCkfgaqoM
PARAM: continue=https://accounts.google.com/o/oauth2/auth?zt=ChRsWFBwd2JmV1hIcDhtU
z4gAAAAAUy4_qD7Hbfz38w8kxnaNouLcRiD3YTjX
PARAM: service=lso
PARAM: dsh=-7381887106725792428
PARAM: _utf8=â
PARAM: bgresponse=js_disabled
PARAM: pstMsg=1
PARAM: dnConn=
PARAM: checkConnection=
PARAM: checkedDomains=youtube
POSSIBLE USERNAME FIELD FOUND: Email=aamir-the-security-guy@gmail.com
POSSIBLE PASSWORD FIELD FOUND: Passwd=Thundercats-Rocks!
PARAM: signIn=Sign+in
PARAM: PersistentCookie=yes
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```

By the Numbers

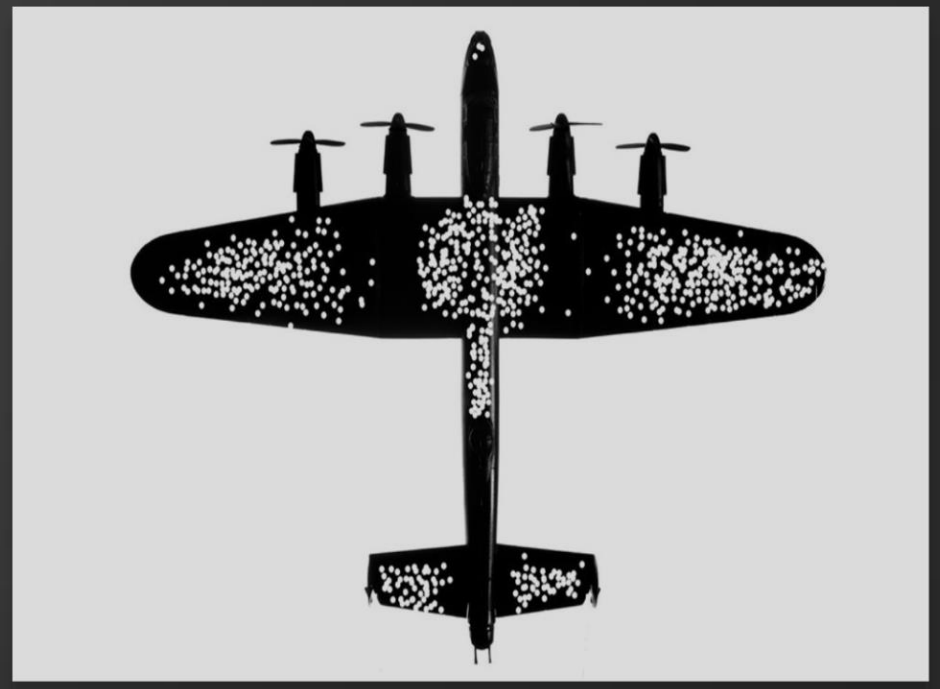
WHY DO WE FAIL?

EVERYONE IS TRYING TO GET AHEAD OF SECURITY

- We often buy the right products for the wrong reasons.
- We are trying to meet the requirements and not solve problems.
- We fall into traps of compliance or reactionary response.

HOW DO WE SUCCEED?

There is no Winter in the city of hope



- During World War II, the British many of planes to German anti-aircraft fire.
- They decided to add heavy armor to mitigate the risk of them being shot down
- They counted the bullet holes on their plane and decided to add extra armor in the areas that were damaged the most
- Most bullet holes were found on the wings
- Hungarian-born mathematician Abraham Wald explained at the time if a plane makes it back safely even though it has, say, a bunch of bullet holes in its wings, it means that bullet holes in the wings aren’t very dangerous.

PERSONAL RECOMMENDATIONS FOR YOUR TEAM

THANK YOU

alakhani@me.com

Aamir Lakhani

Global Senior Security Strategist

ForiGuard Labs

@aamirlakhani

www.fortiguard.com