

CYBER FINANCIAL

SECURITY



HELLO!

I am Francis Nwokelo

I am here because I am NextGen fellow at ICANN60  
in Abu Dhabi.

You can find me at  
[emperorfin4@gmail.com](mailto:emperorfin4@gmail.com)



## REASONS FOR CYBER FINANCIAL INSECURITY

- ✘ The Organizations: e.g. online retailers, banks, etc.
- ✘ The Internet Community: e.g. online shoppers, website visitors, etc
- ✘ The Cyber Threat Actors: e.g. hackers, phishing attackers, etc



# THE ORGANIZATIONS

E.g. online retailers, banks, etc.



More than 90 percent of corporate executives said they cannot read a cybersecurity report and are not prepared to handle a major attack.

*- a Nasdaq's survey*



I think the most shocking statistic was really the fact that the individuals at the top of an organization – executives like CEOs and CIOs, and even board members – **didn't feel personally responsible for cybersecurity or protecting the customer data.**

*– Dave Damato, chief security officer  
at Tanium*



The findings came at a time  
when companies around  
the world are **losing \$445  
billion due to cybercrime**  
(2015).

*- Center for Strategic and  
International Studies*



The frequency and severity of cyber penetrations, as well as the sophistication of hackers, has increased dramatically. **What has not kept pace with that is the education level, the understanding of the impact of cyber across all industries.**

*- Lou Modano, chief information security officer at Nasdaq*





A vast majority of  
the **businesses think**  
that they are at risk  
of **hacking threats.**

*- 2017 Thales Data Threat Report*



65 percent of **Banks**  
failed the 2017 Online  
**Security Test** by  
Online Trust Alliance.

*- Online Trust Alliance*



Basically, the banks used  
the move online as **an  
opportunity to dump the  
fraud risk on the customer.**

*– Ros Anderson, cyber security expert  
and Prof. of security engineering*



Crucially, and contrary to what you will find in the banks' marketing materials, **if you fall victim to an online fraud the chances are you will never see your money again.**

*– Theguardian.com*

2.

# THE INTERNET COMMUNITY

E.g. online shoppers, website visitors, etc



The internet community has been trained to "look for the padlock" in their browser before submitting sensitive information to websites, such as passwords and credit card numbers. However, a displayed padlock alone does not imply that a site using TLS (Transport Layer Security) can be trusted, or is operated by a legitimate organization.

- *Netcraft*



The more people know  
about the risks of fraud and  
how to protect themselves,  
the less likely they are to  
become a victim.

– *A British Bankers' Association*

3.

# THE CYBER THREAT ACTORS

E.g. hackers, phishing attackers, etc





88 percent of hackers can break through cybersecurity defences and into the systems they are targeting within 12 hours. More than 80 percent say they can identify and steal valuable information within a further 12 hours, but the chances are that the breach will not be discovered for hundreds of days.

*- Nuix's Research*



Data breaches will take an average of 250–300 days to detect – if they are ever detected at all – but most attackers say that they can break in and steal target data within the first 24 hours.

– *Chris Pogue, chief information security officer at Nuix*



Cyber attackers  
are one step ahead  
of the defenders.

- *Security Experts*



## SUMMARY OF CYBER FINANCIAL INSECURITY

- ✗ Executives don't feel personally responsible for cybersecurity
- ✗ Businesses think that they are at risk of hacking threats
- ✗ Consumers have been taught to associate the presence of a valid SSL (Secure Socket Layer) certificate with an increased level of assurance without knowing that phishing attacks can make use of SSL certificates
- ✗ Hackers are one step ahead of cybersecurity

# THE WAY FORWARD





# ONLINE FINANCIAL DATA PROTECTION PROCESS





# WHAT | WHO | HOW

## The What – RESEARCH:

The “What” involves finding out *what* the business is actually all about. Is the website or business truly what you think it is? Hence, **RESEARCH**.

## The Who – SSL/TLS

The “Who” is all about finding out *who* is actually behind the domain name of the website you want to transact on. Does the website have a valid encrypted connection? Hence, **SSL/TLS**.

## The How – PCI DSS

The “How” is all about finding out *how* serious the business or website you want to transact on takes security. How does the business protect customers’ financial data that was given to them. Hence, **PCI DSS (Payment Card Industry Data Security Standard)**.



RESEARCH!!!

*You don't want to lose your hard earned money. Do you?*



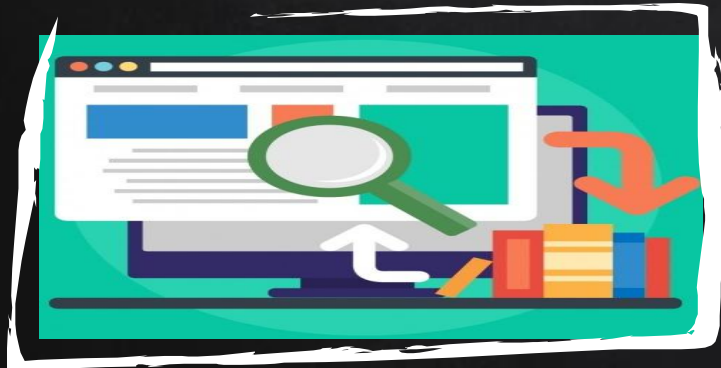


# RESEARCH!!!



**REVIEWS:** Search for what people are saying about the website you want to transact on with keywords like “eBay Reviews” on search engines.

E.g. <https://www.google.com>



**WHOIS LOOKUP:** Find out who’s name and contact info the domain was registered with as well as the domain registrar, website hosting server and location.

E.g. <http://www.ipaddress.com>



# SSL/TLS

*It's all about trust! Not just encrypted connection.*



# SECURE SOCKET LAYER/TRANSPORT LAYER SECURITY (SSL/TLS)

## 3 DIFFERENT ASSURANCE LEVELS OF SSL CERTIFICATES PROVIDED BY CERTIFICATE AUTHORITIES (CA)

### **Domain Validated (DV) SSL:**

CAs only have to check that the certificate's applicant controls the domain name contained in a DV certificate. These certificates are typically the cheapest option, and can be had for free or be purchased for less than \$10.

### **Organization Validated (OV) SSL:**

In addition to validating the domain name in the certificate, the identity of the person or organization applying for an OV certificate is also verified by the certificate authority and included in the certificate.

### **Extended Validated (EV) SSL:**

Like OV certificates, the identity of the organization applying for an EV certificate is verified by the certificate authority. However, the verification is more stringent.



DV certificates, such as one from **Let's Encrypt**, are often issued completely automatically within minutes, **making it easy for fraudsters to obtain DV certificates for deceptive domain names.**

*- Netcraft*



Several certificate authorities offer free trial certificates with shorter validity periods such as 30 and 90 day certificates, which **have been used by a number of SSL phishing attacks**. The short validity periods are ideal for fraudsters as phishing attacks themselves typically have short lifetimes.

*- Netcraft*



EV certificates are only issued by  
CAs after a rigorous identity  
verification process and **provide**  
**the highest level of authentication**  
**available for consumers to validate**  
**the website owner's legitimacy.**

- ?



# DV SSL CERTIFICATES


*Why you must not transact on a website with DV SSL like Let's Encrypt*

21,852 SSL

Let's Encrypt has issued a total of 21,852 SSL certificates containing the word "PayPal" as of October 18th, 2017

17,793 SSL

Let's Encrypt has issued a total of 17,793 SSL certificates containing the word "AppleID" as of October 18th, 2017

96.7% 

Based on a random sample, 96.7% of these certificates were intended for use on phishing sites





# JUST A FEW SCREENSHOTS

https://crt.sh/?Identity=paypal%25&iCAID=16418 Search

**crt.sh Identity Search**

Criteria Identity LIKE 'paypal%'; Issuer CA ID = 16418

Issuer Name	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3			
Certificates (21,852)	1 to 100 <a href="#">Next</a>			
	crt.sh ID	Not Before	Not After	Subject Name
	<a href="#">234209837</a>	2017-10-18	2018-01-16	CN=accounts-manage.paypal-security-update.cf

https://crt.sh/?Identity=appleid%25&iCAID=16418 Search

**crt.sh Identity Search**

Criteria Identity LIKE 'appleid%'; Issuer CA ID = 16418

Issuer Name	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3			
Certificates (17,793)	1 to 100 <a href="#">Next</a>			
	crt.sh ID	Not Before	Not After	Subject Name
	<a href="#">234188073</a>	2017-10-18	2018-01-16	CN=appleid.apple.com-cuenta-de-servicio-id6624.org
	<a href="#">234187541</a>	2017-10-18	2018-01-16	CN=appleid-service-inc.com
<a href="#">234184321</a>	2017-10-18	2018-01-16	CN=www.anukuanumuasdewe.com	

More info at: <https://crt.sh/?Identity=paypal%25&iCAID=16418> and <https://crt.sh/?Identity=appleid%25&iCAID=16418>



To determine the ratio of phishing sites vs. legitimate ones, we took a random sample of 1000 certificates and reviewed them by hand. For the vast majority of certificates, the hostname made the purpose of the site clear. We avoided false positives by labeling sites as “legitimate” when we were unsure, and visited the sites when necessary. **In our sample we found a phishing rate of 96.7%.**  
– *TheSSLStore.com, Rapid Web Services, LLC*



Both cases show that nearly all "PayPal" certificates being issued by Let's Encrypt are intended for phishing, and legitimate users make up only a single-digit share.

- *TheSSLStore.com, Rapid Web Services, LLC*

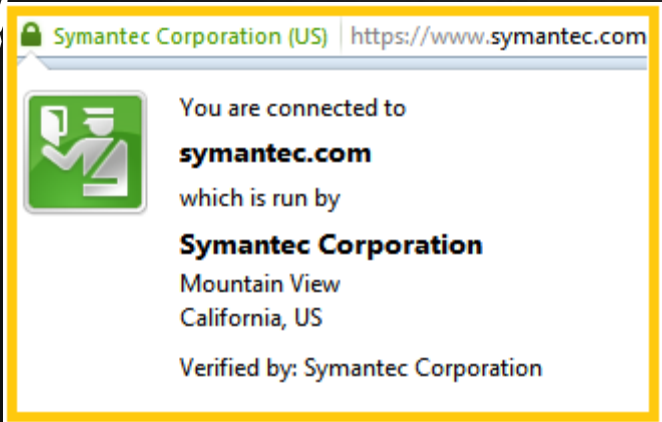


# EV SSL CERTIFICATES

*Try to identify that the website SSL certificate is EV before transacting on it.*




## HOW TO KNOW IF A WEBSITE USES EV SSL




- ✗ **https://** – A URL that starts with https instead of http
- ✗ **Padlock icon** in the address bar
- ✗ **“Secure”** or **Green bar**



# RECOMMENDATION AND MORE INFO

Limited (GB) | <https://crt.sh?q=ebay.com> 

**crt.sh** Identity Search  [Group by Issuer](#)

Criteria Identity = 'ebay.com'

<a href="#">crt.sh ID</a>	<a href="#">Logged At</a> ↑	<a href="#">Not Before</a>	<a href="#">Issuer Name</a>
<a href="#">203211098</a>	2017-09-02	2017-08-31	<a href="#">C=US, O=Symantec Corporation, OU=Symantec Trust Network, CN=Symantec Class 3 Secure Server CA - G4</a>
<a href="#">202029055</a>	2017-08-31	2017-08-31	<a href="#">C=US, O=Symantec Corporation, OU=Symantec Trust Network, CN=Symantec Class 3 Secure Server CA - G4</a>
<a href="#">160442560</a>	2017-06-23	2017-06-24	<a href="#">C=US, O=Symantec Corporation, OU=Symantec Trust Network, CN=Symantec Class 3 Secure Server CA - G4</a>

Go to: <https://crt.sh>



# RECOMMENDATION AND MORE INFO (CONTD.)

## Certificate:

Data:

Version: 3 (0x2)

### Serial Number:

72:90:cf:a7:0a:32:56:77:af:a8:7a:ef:c6:91:db:a2

Signature Algorithm: sha256WithRSAEncryption

### Issuer:

commonName = Symantec Class 3 Secure Server CA - G4  
organizationalUnitName = Symantec Trust Network  
organizationName = Symantec Corporation  
countryName = US

### Validity

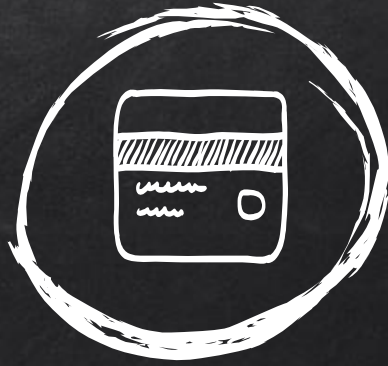
Not Before: Aug 31 00:00:00 2017 GMT

Not After : Jun 22 23:59:59 2018 GMT

### Subject:

commonName = pages.ebay.com  
organizationalUnitName = Site Operations  
organizationName = eBay, Inc.  
localityName = San Jose  
stateOrProvinceName = California  
countryName = US

Subject Public Key Info:



# PCI DSS

*Is website PCI DSS (payment card industry data security standard) compliant?*





SSL Secure  
Connection **Isn't**  
Secure Website.

- ?



## WEBSITE USING INTERNAL OR EXTERNAL PAYMENT GATEWAY?

✘ **Visa** : Checkout VISA PCI compliance list at <https://www.visa.com/splisting/searchGrsp.do> and be sure to select “Validation Type” as “PCI DSS”

✘ **MasterCard**: Checkout MasterCard PCI compliance list at [http://www.mastercard.com/us/company/en/whatwedo/complaint\\_providers.html](http://www.mastercard.com/us/company/en/whatwedo/complaint_providers.html)



## WEBSITE NOT ON THE LIST, USING EXTERNAL PAYMENT GATEWAY BUT STILL STORING SOME SENSITIVE DATA

If you must transact on the website that's not on the list but still stores some of your sensitive data and uses external PCI compliant payment gateway, it's risky though but checkout the following:

- ✗ **Builtwith.com:** What is the technology behind the website you want to transact on?
- ✗ **Sucuri.net:** One of the places to checkout vulnerability in the technology/website.

INSTEAD OF A CONCLUSION

# CYBER FINANCIAL SECURITY INITIATIVE

✗ **Why**: More than half of the world's population are yet to access the internet. It would be catastrophic if they are not educated about cyber financial security

✗ **Achievements**: I've been able to educate my community on cyber financial security as they were formally scared of doing businesses over the internet due to cyber fraud.

✗ **How**: I was able to achieve that by educating them without going in much technical details and they became very interested

✗ **Next milestone**: I would like to take it to the state, national or even global level but currently experiencing constraints due to lack of sponsor

✗ **Why should it be sponsored**: There's no shortage of cybersecurity industry reports so I've avoided going down the familiar path of compiling data about incidents that have already taken place or highlighting trends in data breaches – these are clearly the symptoms of a deeper problem. Instead, I'm focusing on educating the internet community about cybersecurity especially in the areas of finance.



THANKS!

Any questions?

You can find me at  
[emperorfin4@gmail.com](mailto:emperorfin4@gmail.com)