Mirazon®

Today's Threat Landscape

Threats, Scams, and Phishing

Friday, September 25th
Rance Reinhardt
Rance.Reinhardt@Mirazon.com
502-240-0404

Rance Reinhardt

Communications for 5 years in the US Army

Network engineer with Mirazon for 5 years

Currently FortiNet, Ruckus, CWNA, MS Certified

Previously Cisco, CompTIA Certified

Previously DoD 8570.01-M IAM Level II

What Hacking REALLY Is

Ponemon INSTITUTE

63% of companies can not monitor off-network endpoints, over half can't determine endpoint compliance status

LACK OF VISIBILITY

Through 2021, **99%** of vulnerabilities exploited will continue to be ones known by security and IT professionals for at least one year.

VULNERABLE ENDPOINTS

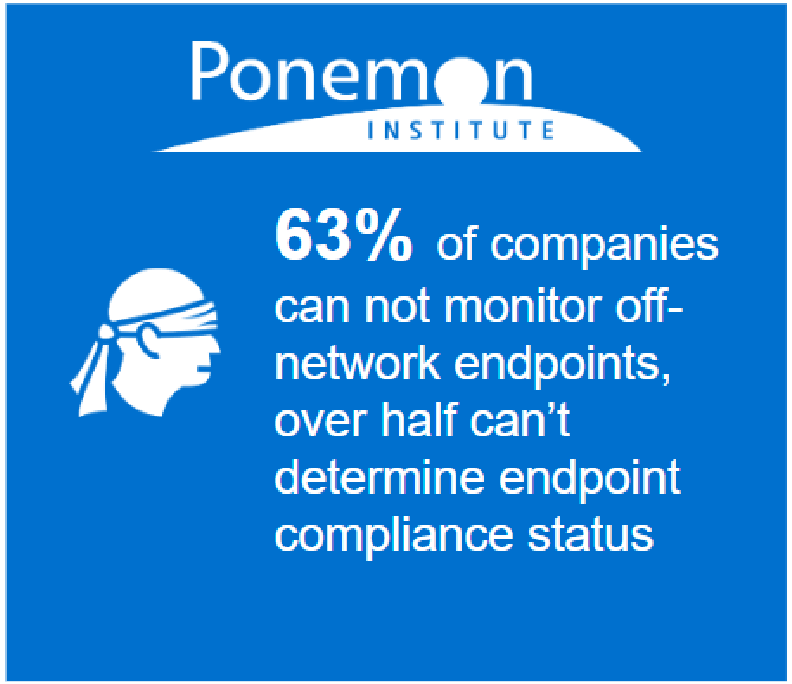
verizon✓

4% of people will click on any phishing campaign

GULLIBLE END USERS

Sources:

1. The Cost Of Insecure Endpoints, Ponemon Institute, 2017
2. Gartner, How to Respond to the 2018 Threat Landscape, Greg Young, 28 November, 2017
3. Breach Investigation Report, Verizon, 2018



Ponemon INSTITUTE

63% of companies can not monitor off-network endpoints, over half can't determine endpoint compliance status

LACK OF VISIBILITY

- Have you identified wants and needs?
- Do you have an established standard?
- Do you have products that can see a client's OS and its installed software?
- Do you have products that can communicate and work together?
- Do you have a deployment plan and goals?

Fabric Agent Use Case

- Risk-based visibility
  - Identify unpatched vulnerabilities with patching options
  - Software inventory for visibility on installed application and versions
- Dynamic access control
- Integrated and automated
  - Integrated with the Security Fabric
  - Automated response to contain incidents
- Compatibility

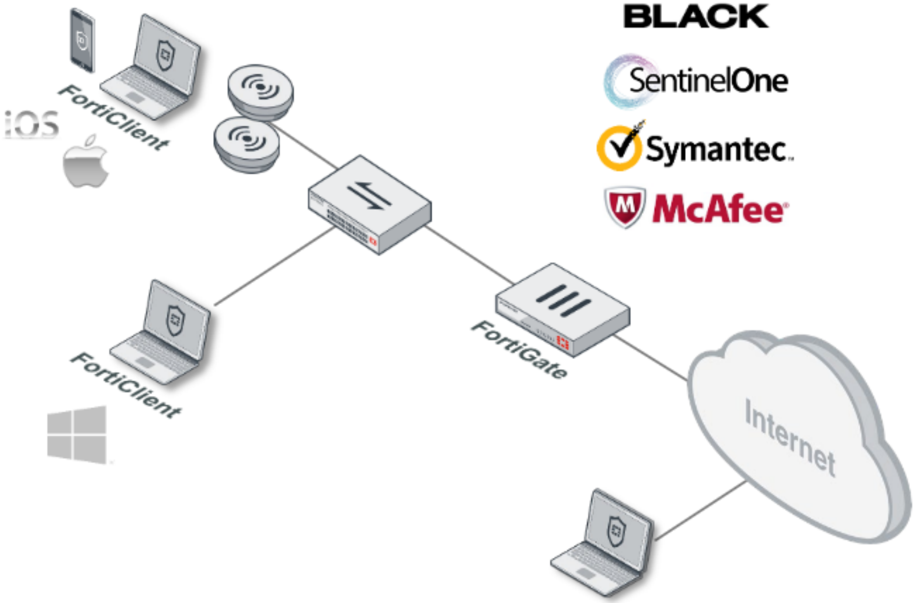
FORTINET Fabric-Ready

CARBON BLACK

SentinelOne

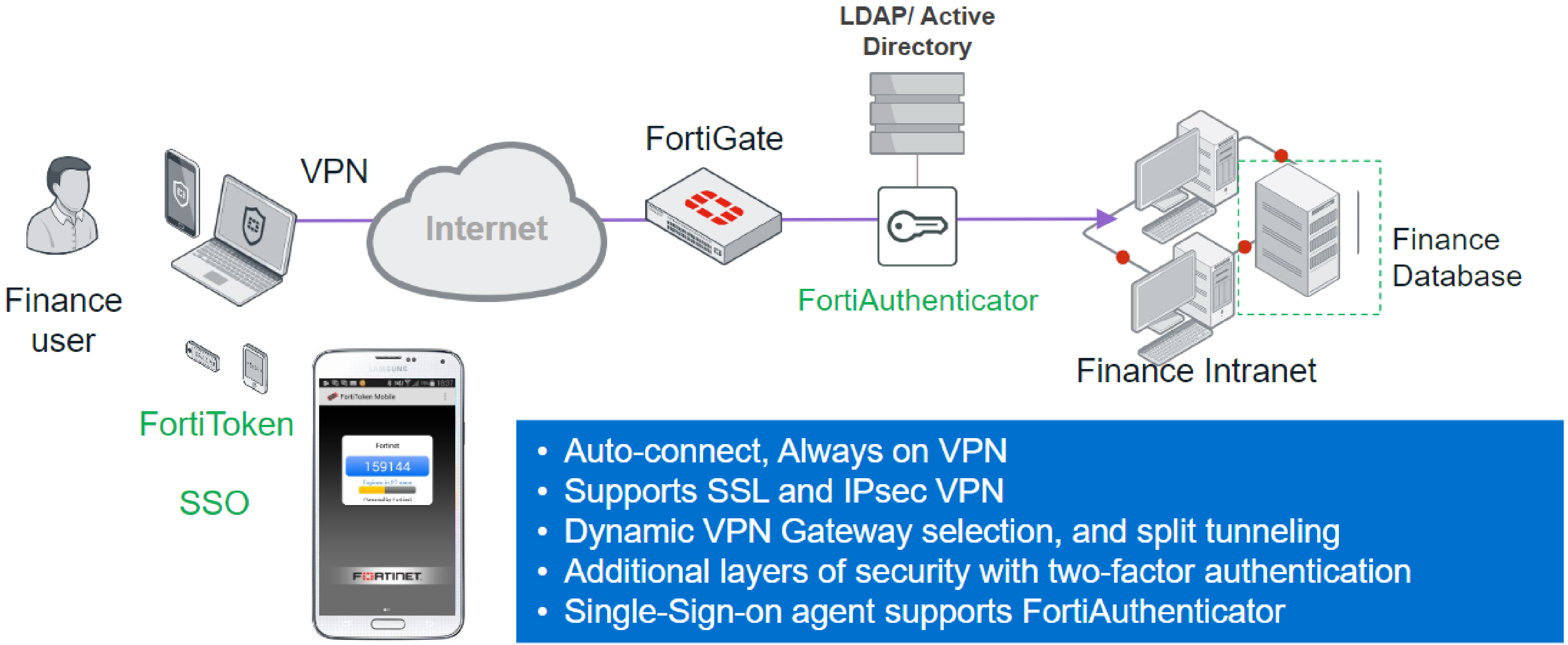
Symantec.

McAfee

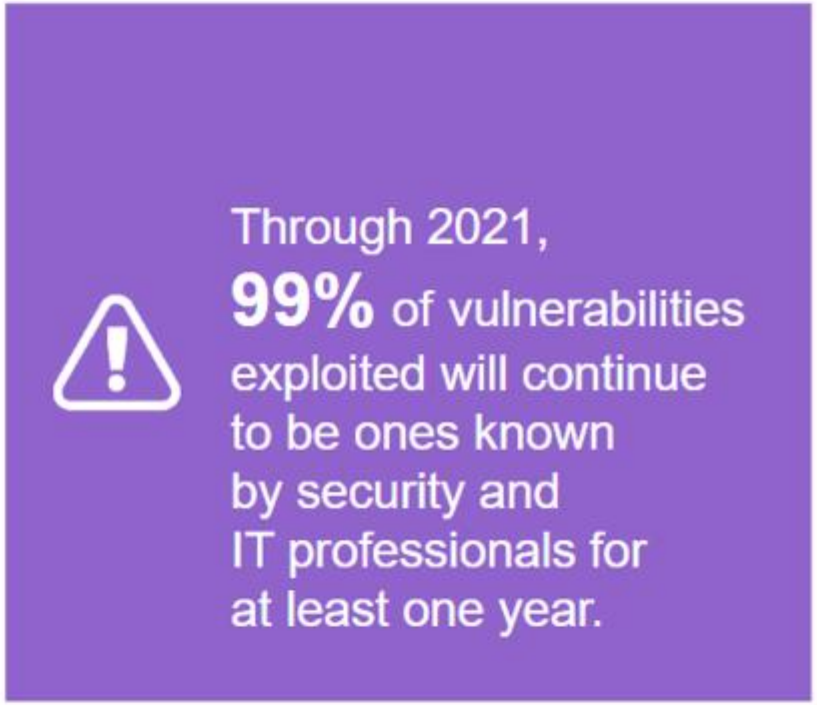


Secure Remote Access

VPN ✚ Two Factor Authentication (2FA) ✚ Single Sign On (SSO)



- Auto-connect, Always on VPN
- Supports SSL and IPsec VPN
- Dynamic VPN Gateway selection, and split tunneling
- Additional layers of security with two-factor authentication
- Single-Sign-on agent supports FortiAuthenticator



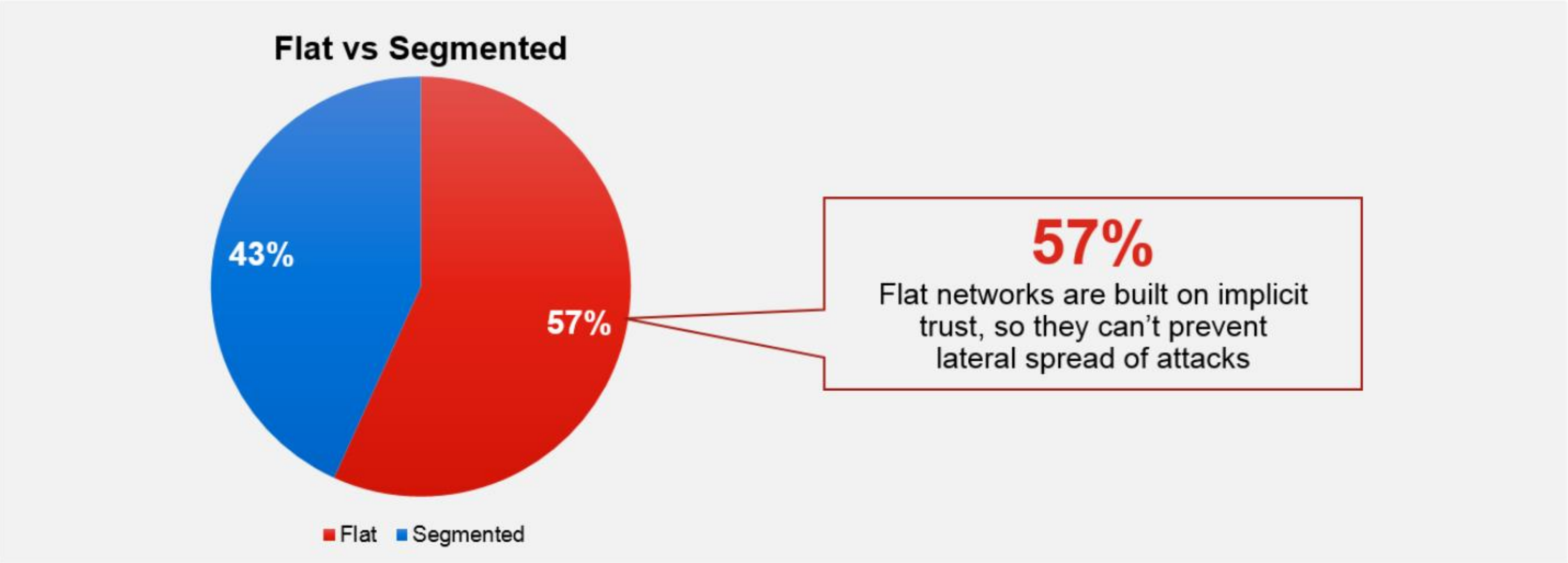
Through 2021, **99%** of vulnerabilities exploited will continue to be ones known by security and IT professionals for at least one year.

VULNERABLE ENDPOINTS

- Your endpoints are everywhere.
- Cloud products are changing the threat landscape and your attack surface.
- DO NOT RELY ON AZURE OR AWS TO PROTECT YOUR ENDPOINTS OR YOUR DATA!

Concern about Cyber Risks Is a Major Inhibitor for Data Center Transformation to the Cloud

… having a flat network further compounds the problem, as they have no ability to prevent attacks



57%
Flat networks are built on implicit trust, so they can't prevent lateral spread of attacks

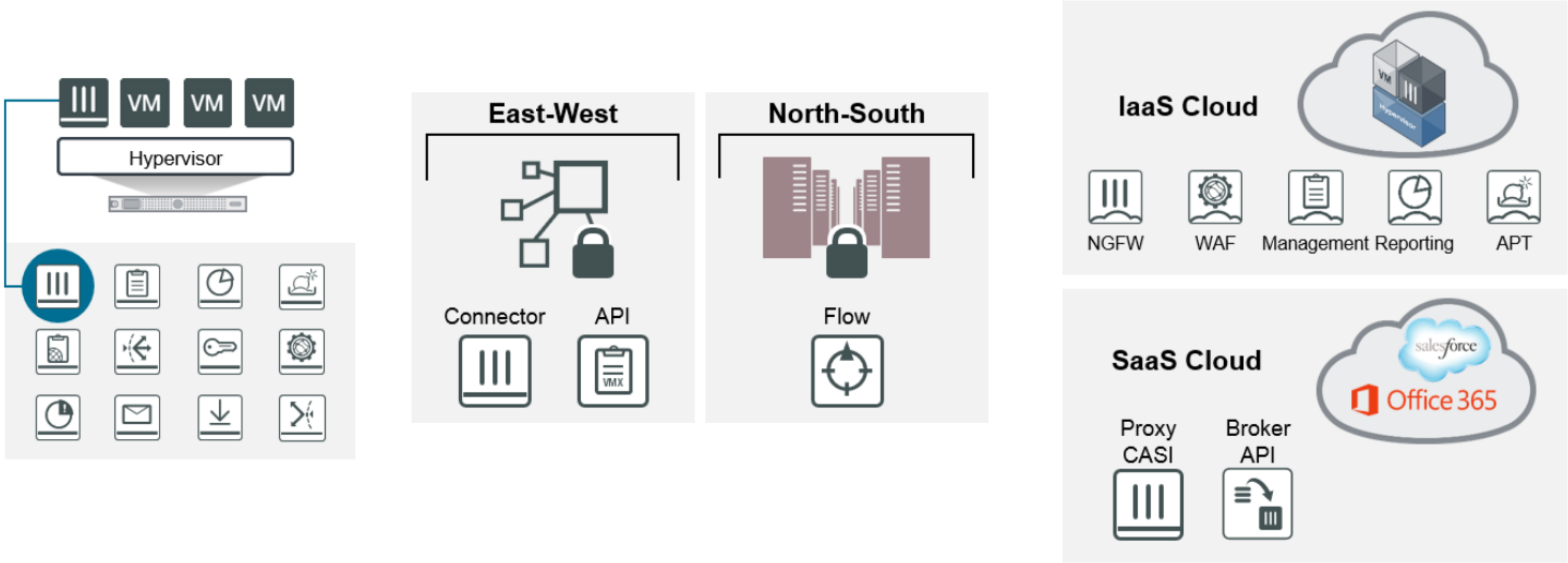
Cloud Security Evolution

Virtualization → Private Cloud ↔ Hybrid ↔ Public Cloud

Hypervisor Port

SDN—Orchestration Integration

On-Demand



VM VM VM

Hypervisor

East-West

Connector

API

VMX

North-South

Flow

IaaS Cloud

VM

NGFW

WAF

Management

Reporting

APT

SaaS Cloud

Proxy CASI

Broker API

salesforce

Office 365

Fortinet Security Fabric Builds from the Core Network

Broad

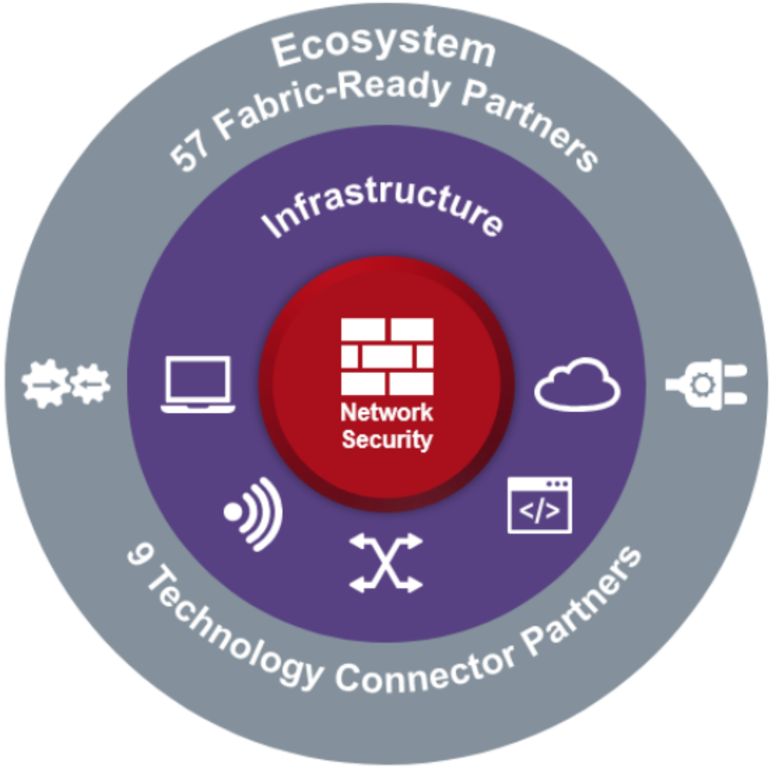
Visibility of the entire digital attack surface

Integrated

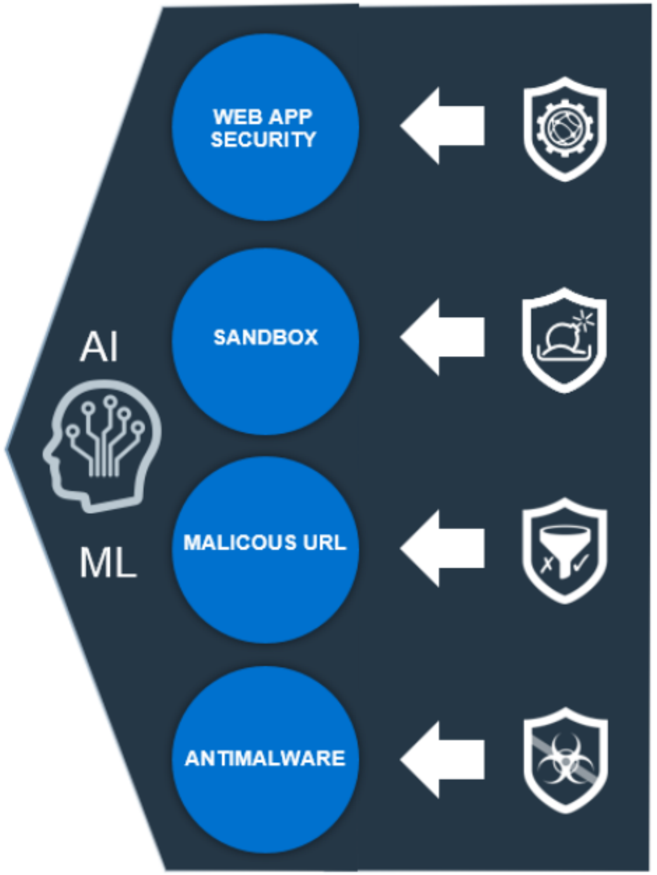
Protection and Detection of Advanced Threats

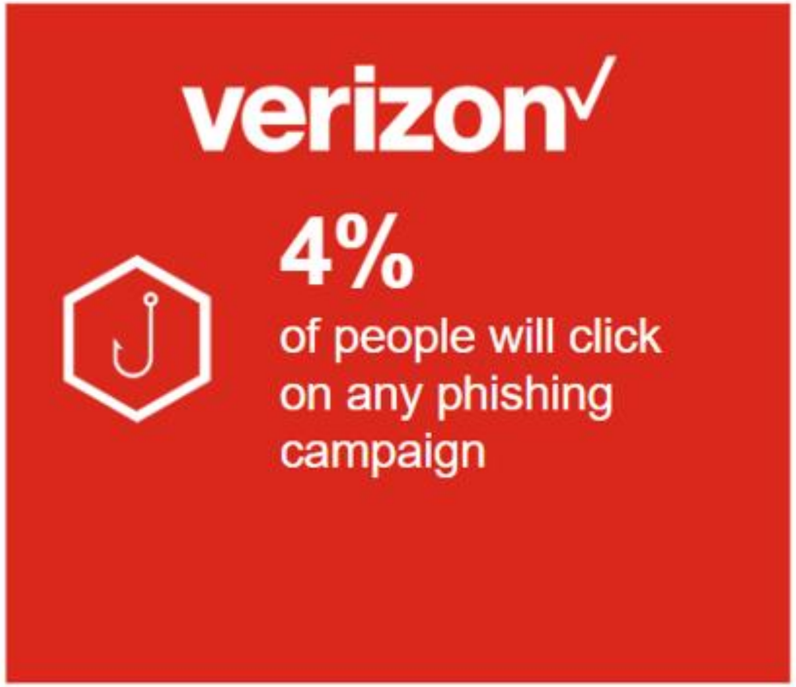
Automated

Operations, Orchestration and Response



Powered by AI





verizon✓

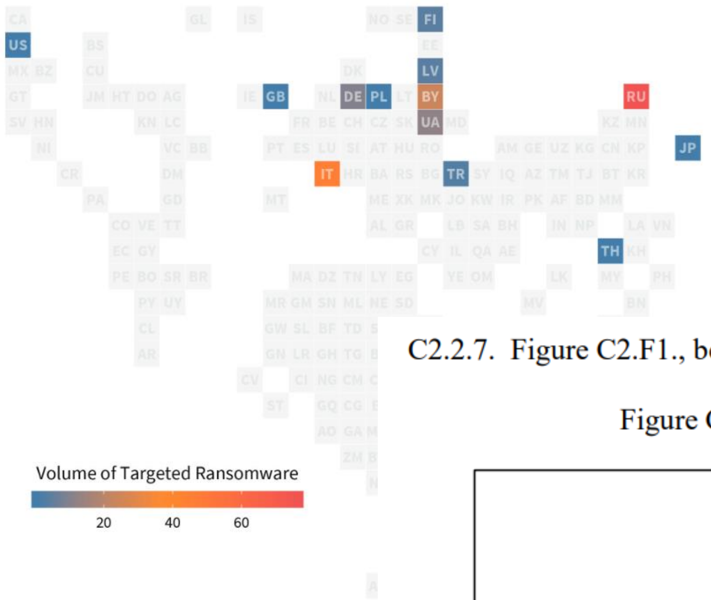
4%

of people will click on any phishing campaign

GULLIBLE END USERS

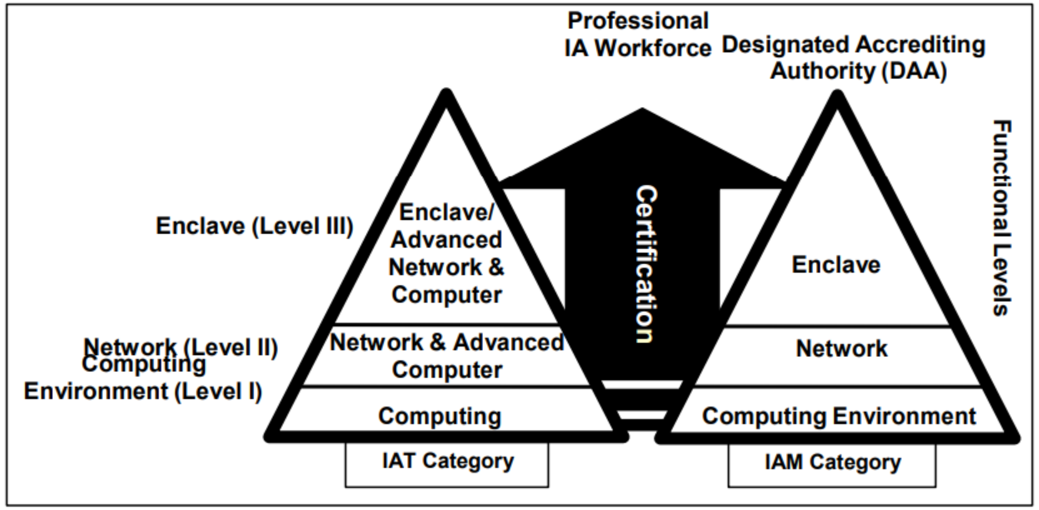
- Do you have regularly scheduled basic security classes for all employees?
- Do you have regularly scheduled advance security classes for IT personnel?
- Do you have a separation of duties policy?
- Have you considered rotation of responsibilities?
- You don’t have the DoD but DISA guidelines are useful.

The DISA and DoD Mindset



C2.2.7. Figure C2.F1., below, provides an overview of the basic IA workforce structure.

Figure C2.F1. Overview of Basic IA Workforce Structure


Professional IA Workforce
Designated Accrediting Authority (DAA)
Functional Levels
Certification
Enclave (Level III)
Enclave/ Advanced Network & Computer
Network (Level II)
Network & Advanced Computer
Computing Environment (Level I)
Computing
IAT Category
Enclave
Network
Computing Environment
IAM Category

Reference Documents
DoD 8570.01-M
DoDD 8140.01

Resource: https://public.cyber.mil

ADVANTAGES of Job Rotation

- Eliminates boredom
- Encourages development
- Give employees a break from strenuous job duties
- Helps you identify where employees work best
- Gives you a backup plan if an employee leaves

DISADVANTAGES of Job Rotation

- Can be costly and time consuming
- Could end up with disgruntled employees
- It won't fix all your problems
- Might not be feasible for some industries
- Your business could suffer

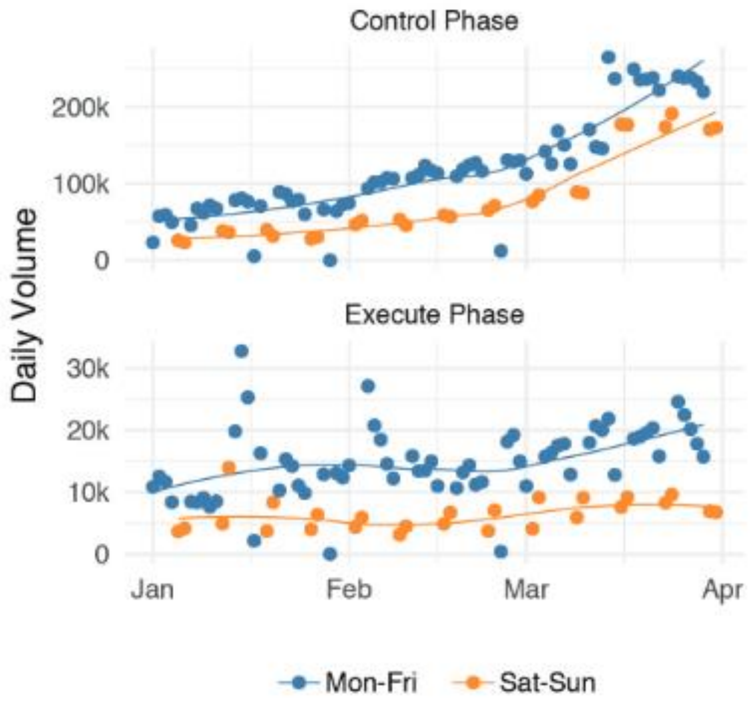
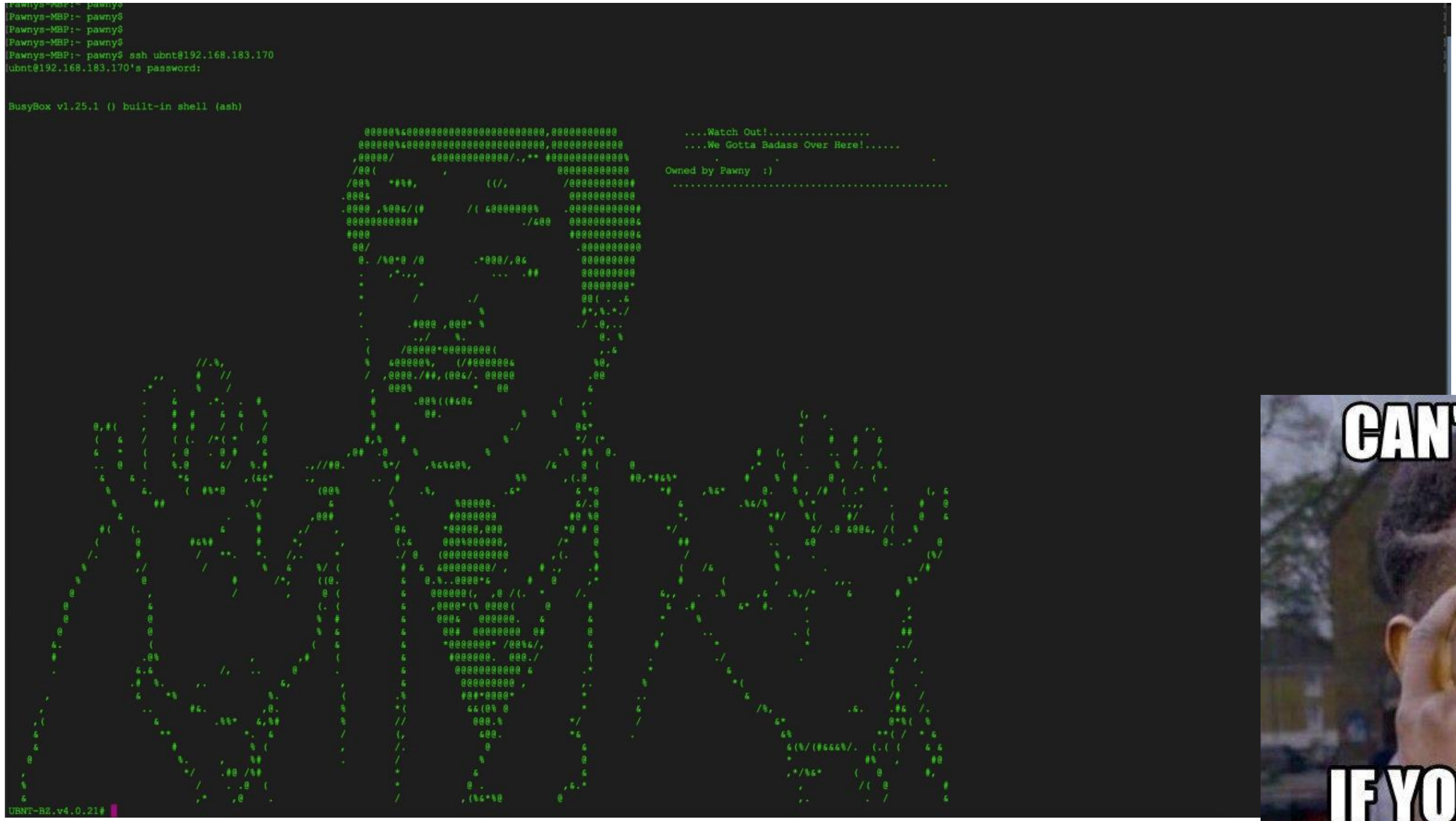


Figure 8: Comparison of web filtering volume for two Cyber Kill Chain phases during weekdays (blue) and weekends (orange).

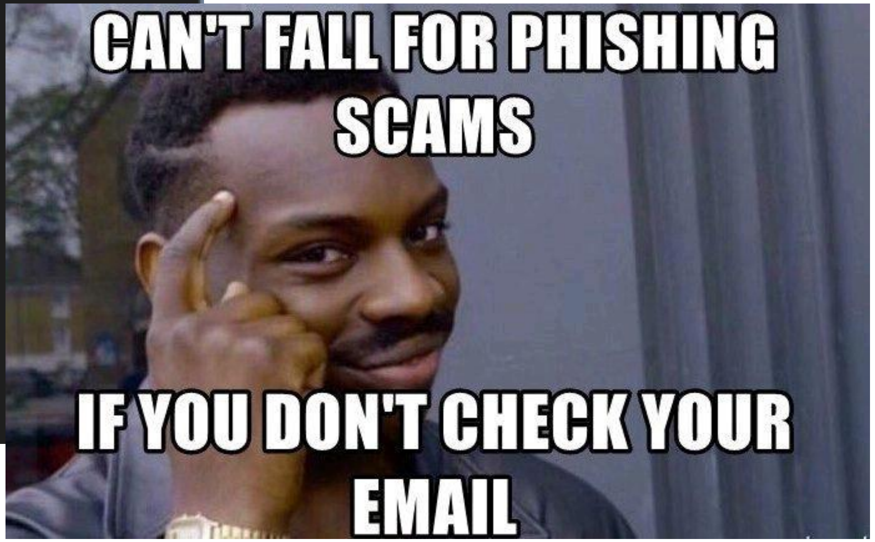
- Hackers/Scammers like to take their afternoons and weekends off too.

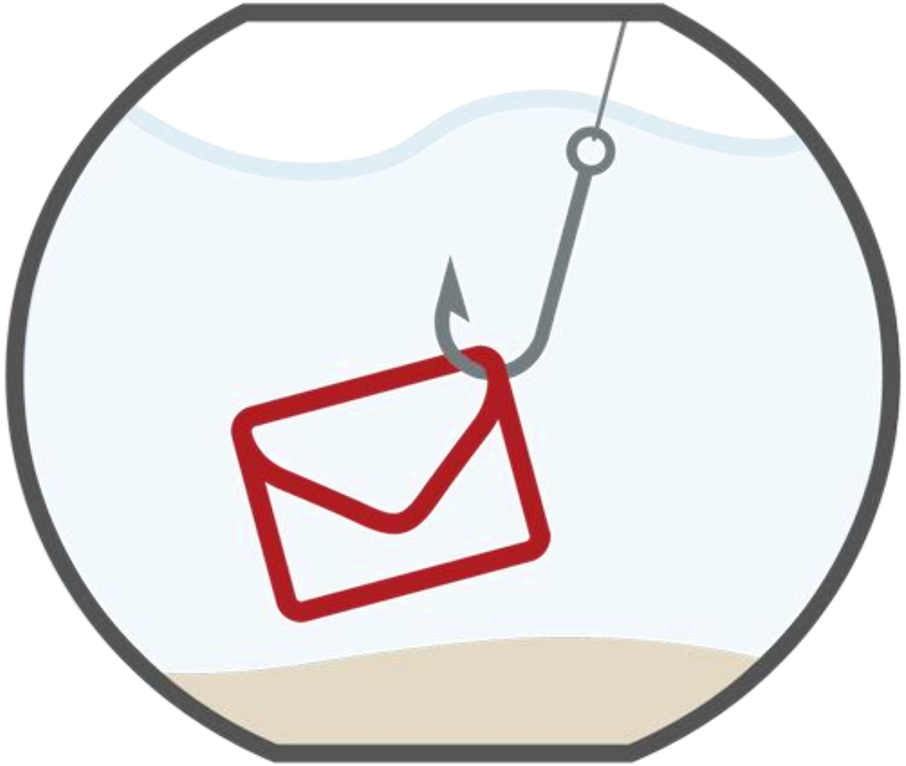
- You are most vulnerable when your employees are at work.

- Hackers/Scammers are typically not who you assumed they are.



```
Pawnys-MBP:~ pawny$
Pawnys-MBP:~ pawny$
Pawnys-MBP:~ pawny$
Pawnys-MBP:~ pawny$
Pawnys-MBP:~ pawny$ ssh ubnt@192.168.183.170
ubnt@192.168.183.170's password:


BusyBox v1.25.1 () built-in shell (ash)

                                   ....Watch Out!.................
                                   ....We Gotta Badass Over Here!......

                                 Owned by Pawny  :)
                                  ..........................................

UBNT-BZ.v4.0.21#
```



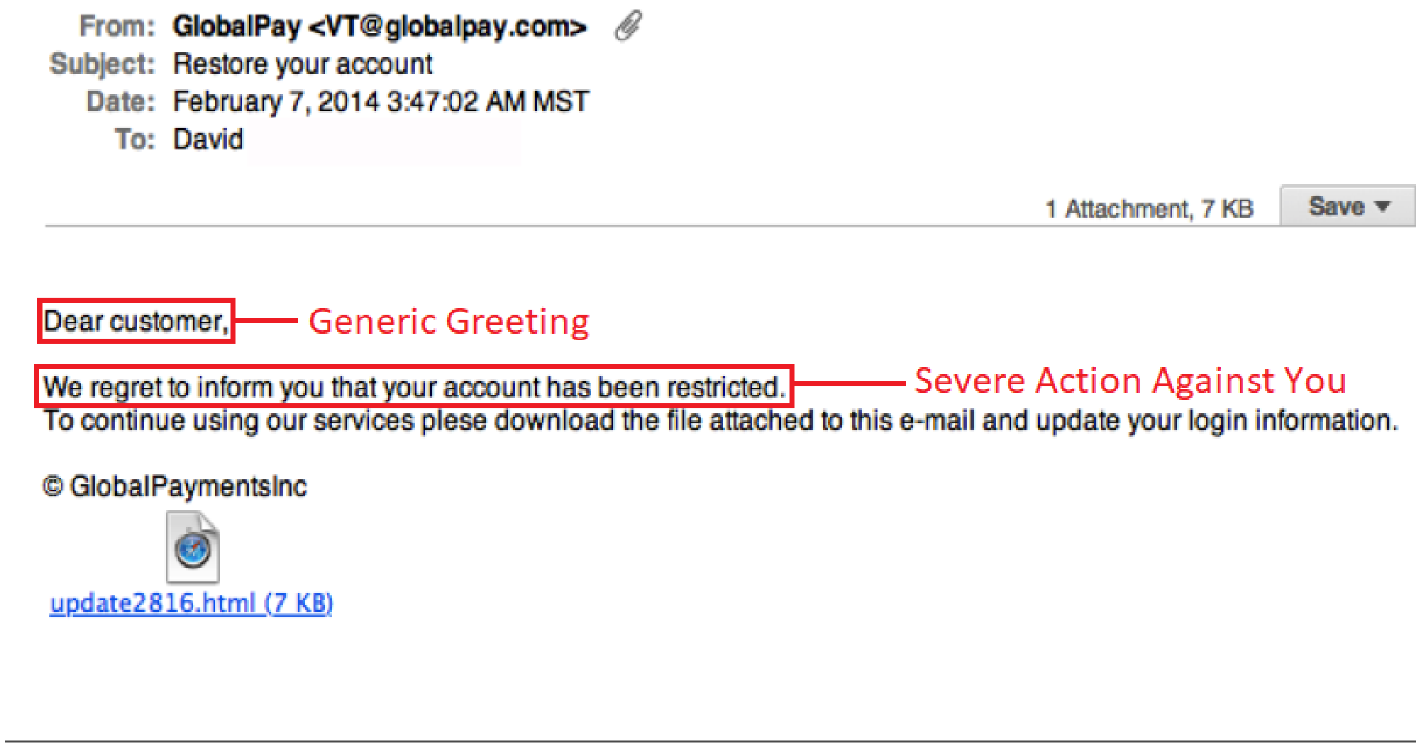


Phishing

Phishing is the fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and financial information.

- 76% of Organizations experienced phishing attacks.
- 16 malicious emails a month per user.
- 92.4% of malware was delivered in email.

According to data from AlertLogic and Symantec's 2018 Internet Threat Report



From: GlobalPay <VT@globalpay.com>
Subject: Restore your account
Date: February 7, 2014 3:47:02 AM MST
To: David

1 Attachment, 7 KB

Dear customer,

We regret to inform you that your account has been restricted.
To continue using our services plese download the file attached to this e-mail and update your login information.

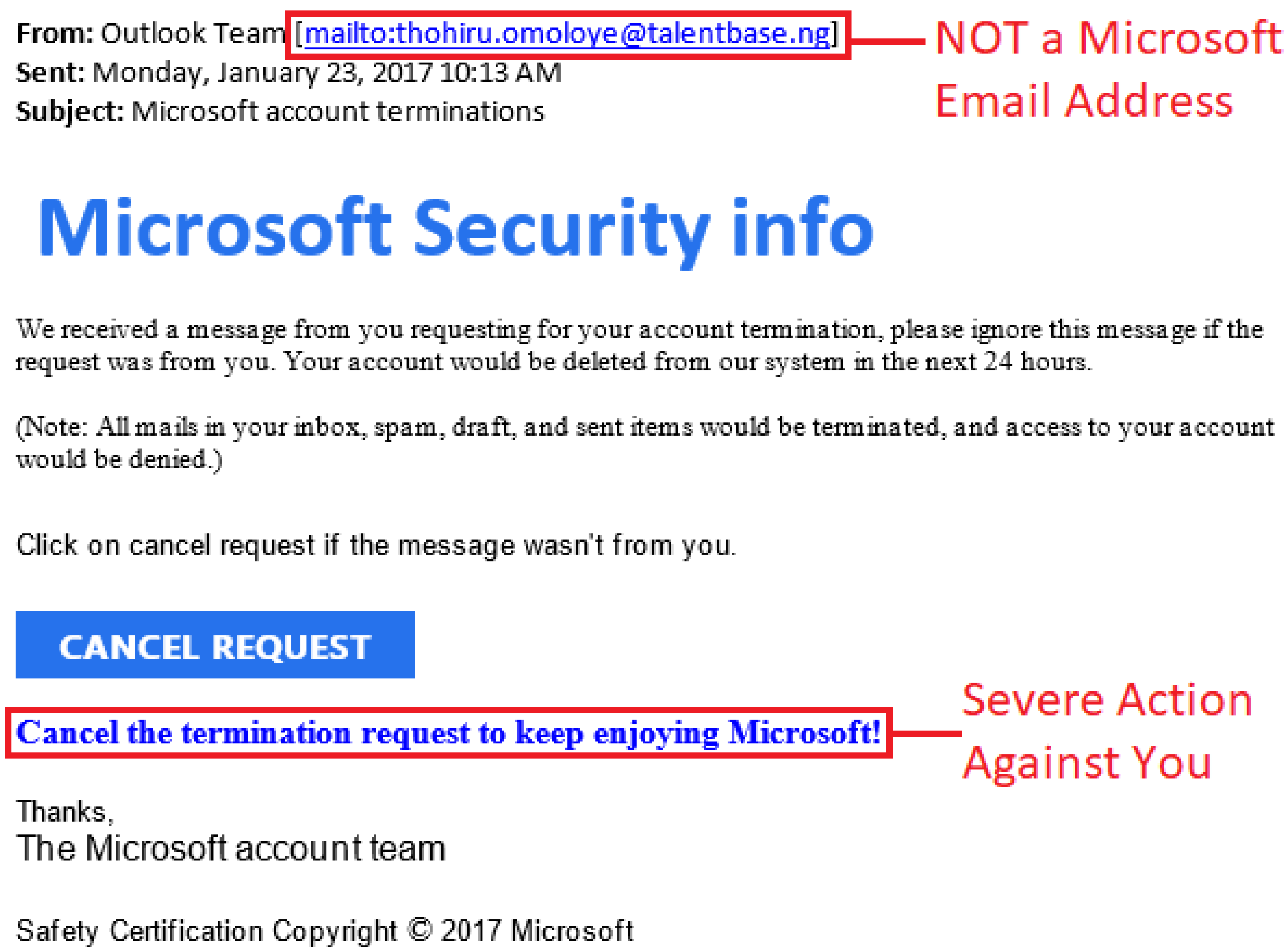
© GlobalPaymentsInc

update2816.html (7 KB)

Generic Greeting

Severe Action Against You

- **Be Discerning of Requests for Highly Sensitive Information**
  - Requests for passwords, financial information, private company data, ETC.
  - If unsure, contact the requester and verify the request
- **Recognize Wrongful Use of Fear and Urgency**
  - Requests asking you to drop everything and fulfil a task immediately usually don't require such urgency
  - Any sort of threats to take severe action against you if requests aren't met are a tell-tale sign of a phishing attempt



From: Outlook Team [mailto:thohiru.omoloye@talentbase.ng]
Sent: Monday, January 23, 2017 10:13 AM
Subject: Microsoft account terminations

NOT a Microsoft Email Address

Microsoft Security info

We received a message from you requesting for your account termination, please ignore this message if the request was from you. Your account would be deleted from our system in the next 24 hours.

(Note: All mails in your inbox, spam, draft, and sent items would be terminated, and access to your account would be denied.)

Click on cancel request if the message wasn't from you.

CANCEL REQUEST

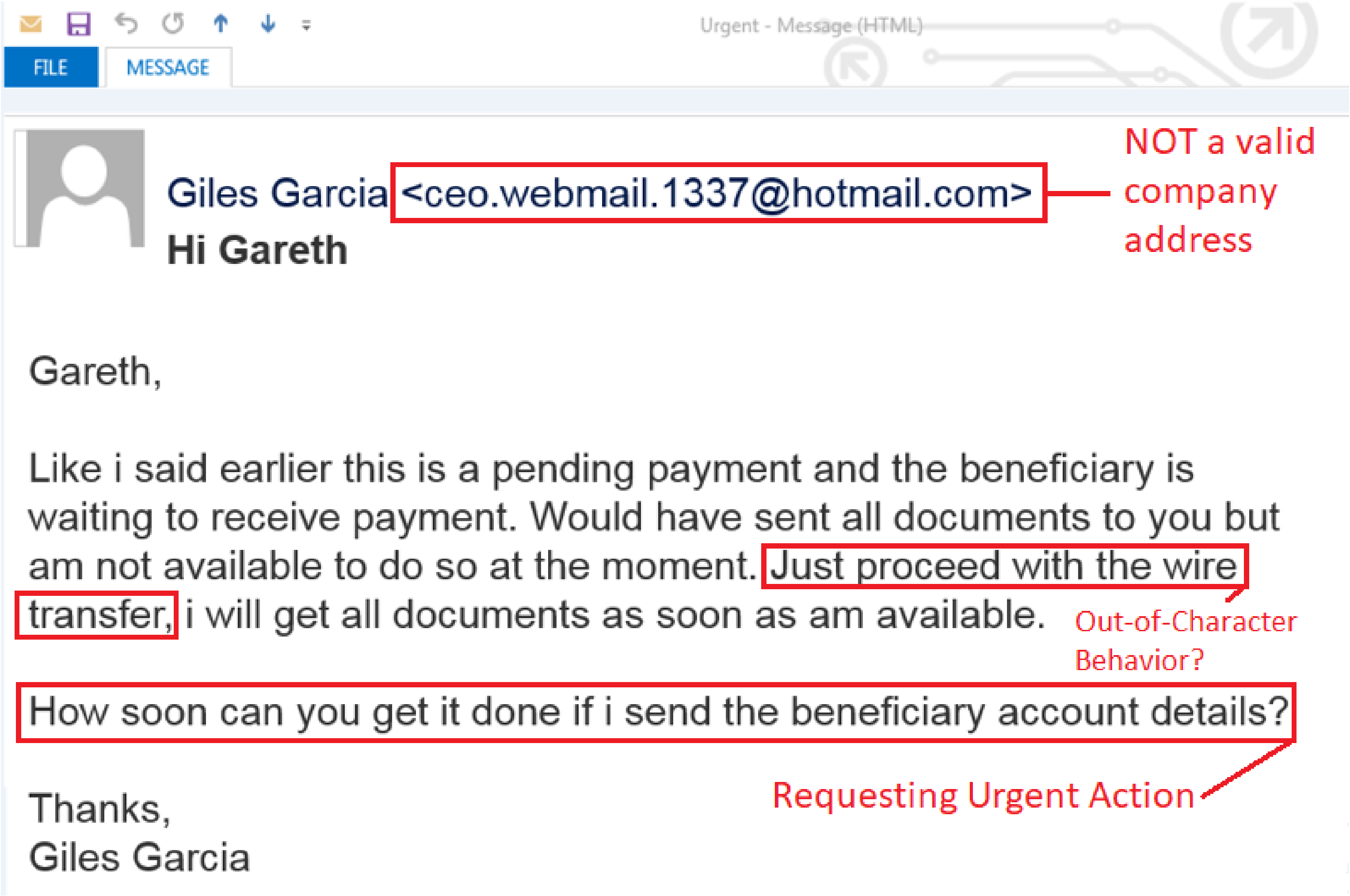
Cancel the termination request to keep enjoying Microsoft!

Severe Action Against You

Thanks,
The Microsoft account team

Safety Certification Copyright © 2017 Microsoft

- **Be Observant**
  - Be on the Lookout for Out-of-Character Behavior
  - Beware impersonal or generic greetings, such as “Dear Customer” or “Hello User”
  - Look for misspellings and unnecessary capitalization or punctuation
  - Double check any URLs included in the email, as well as the sender’s address
    - Hovering over the URL / sender’s address will reveal it’s true identity



Giles Garcia <ceo.webmail.1337@hotmail.com>

Hi Gareth

Gareth,

Like i said earlier this is a pending payment and the beneficiary is waiting to receive payment. Would have sent all documents to you but am not available to do so at the moment. Just proceed with the wire transfer, i will get all documents as soon as am available.

How soon can you get it done if i send the beneficiary account details?

Thanks,
Giles Garcia

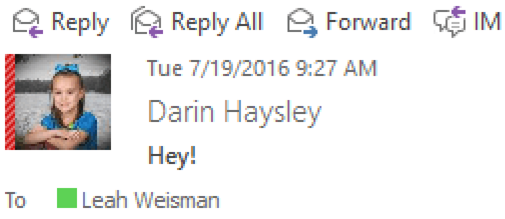
NOT a valid company address

Out-of-Character Behavior?

Requesting Urgent Action

Also note the lack of capitalization on the 'i's and the poor grammar in some areas.

A real sender in your organization would be trusted and outlook typically masks the email address with the contact's name.

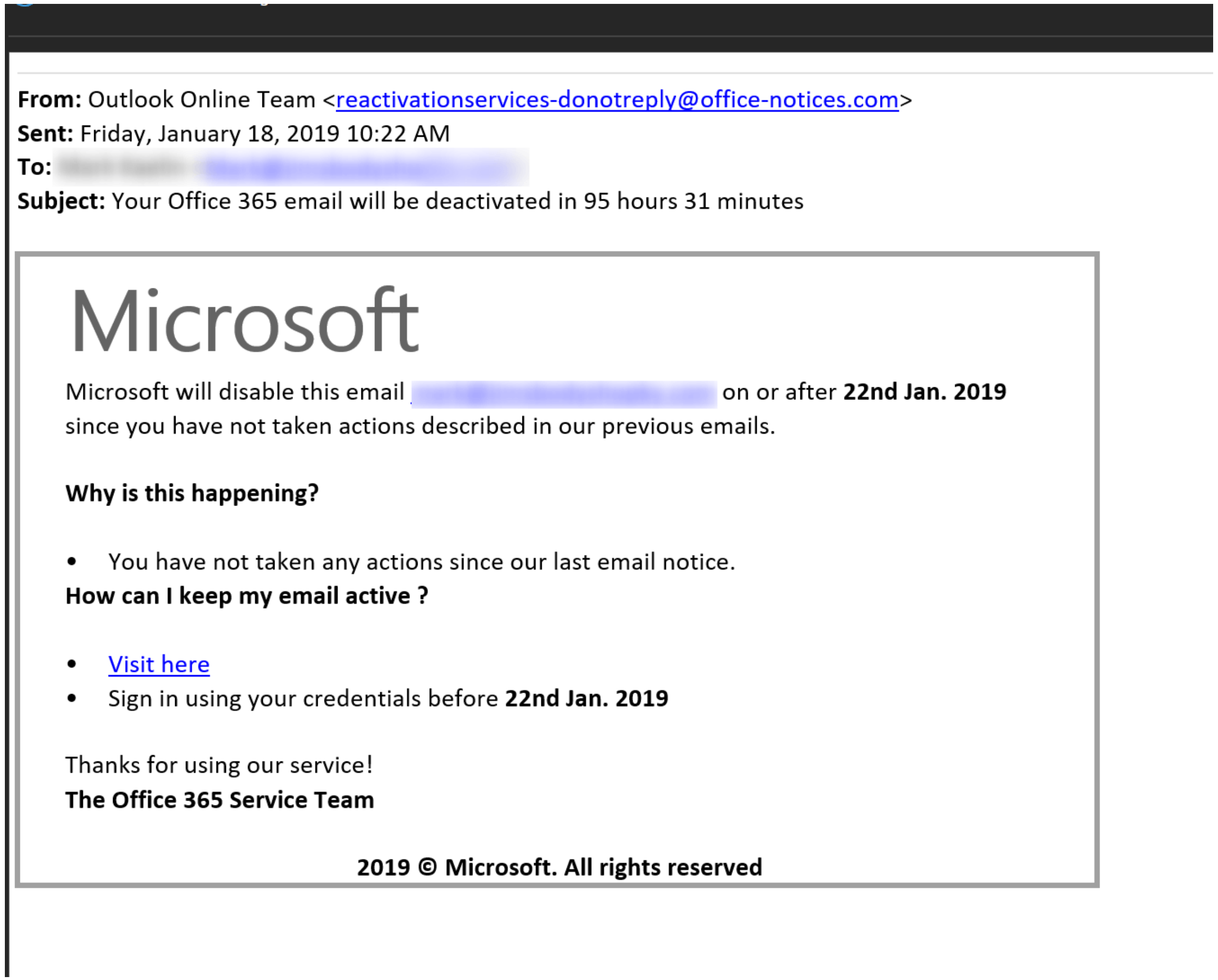


Tue 7/19/2016 9:27 AM

Darin Haysley

Hey!

To 🟩 Leah Weisman



From: Outlook Online Team <reactivationservices-donotreply@office-notices.com>
Sent: Friday, January 18, 2019 10:22 AM
To: [redacted]
Subject: Your Office 365 email will be deactivated in 95 hours 31 minutes

Microsoft

Microsoft will disable this email [redacted] on or after **22nd Jan. 2019** since you have not taken actions described in our previous emails.

Why is this happening?

- You have not taken any actions since our last email notice.

How can I keep my email active ?

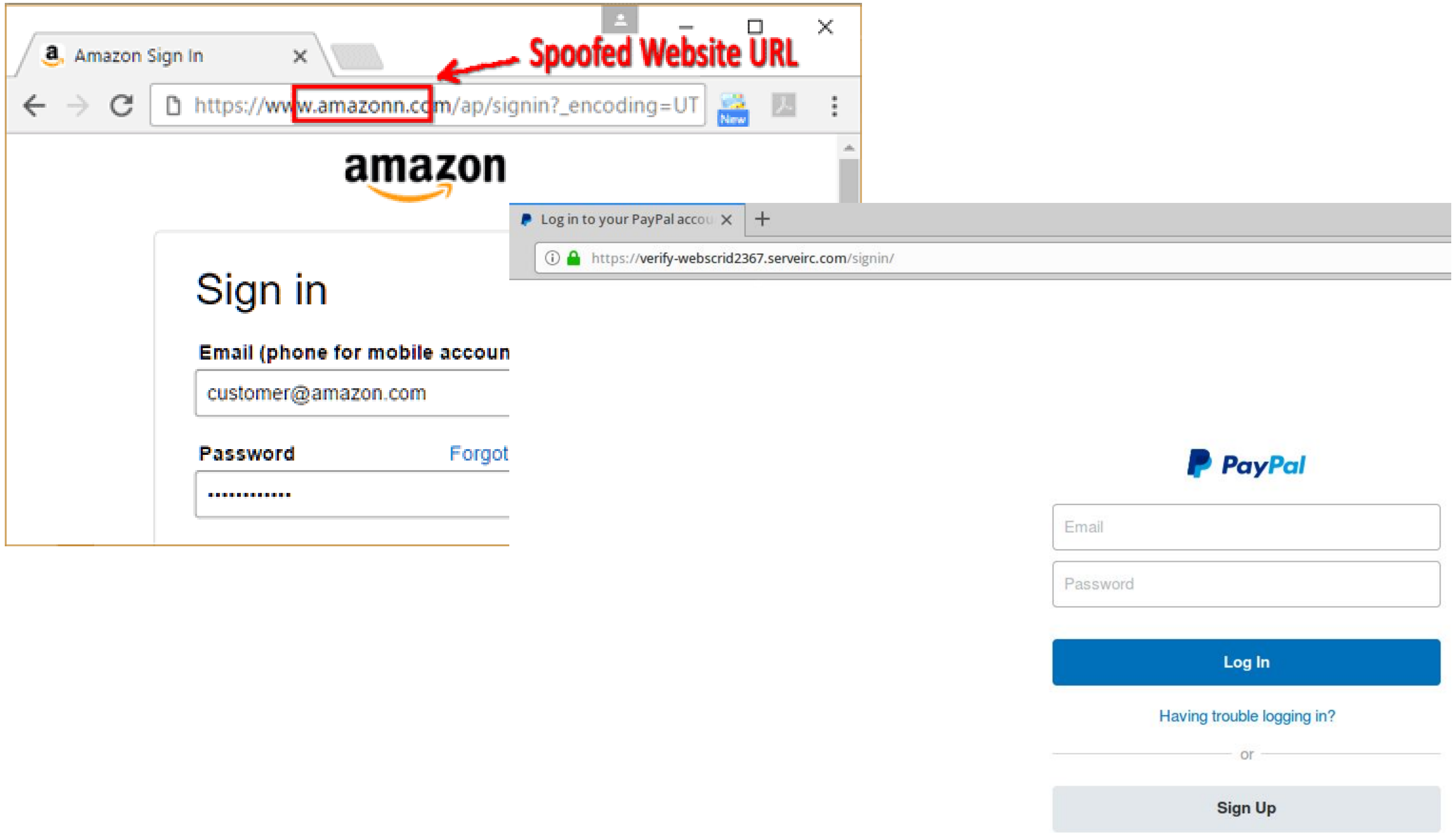
- Visit here
- Sign in using your credentials before **22nd Jan. 2019**

Thanks for using our service!
The Office 365 Service Team

2019 © Microsoft. All rights reserved

All account related Microsoft emails will only come from @Microsoft.com.

If you receive anything like this, even if you believe it's real it best to inform you IT Support.



Spoofed Website URL

https://www.amazonn.com/ap/signin?_encoding=UT

Email (phone for mobile accoun

customer@amazon.com

Password

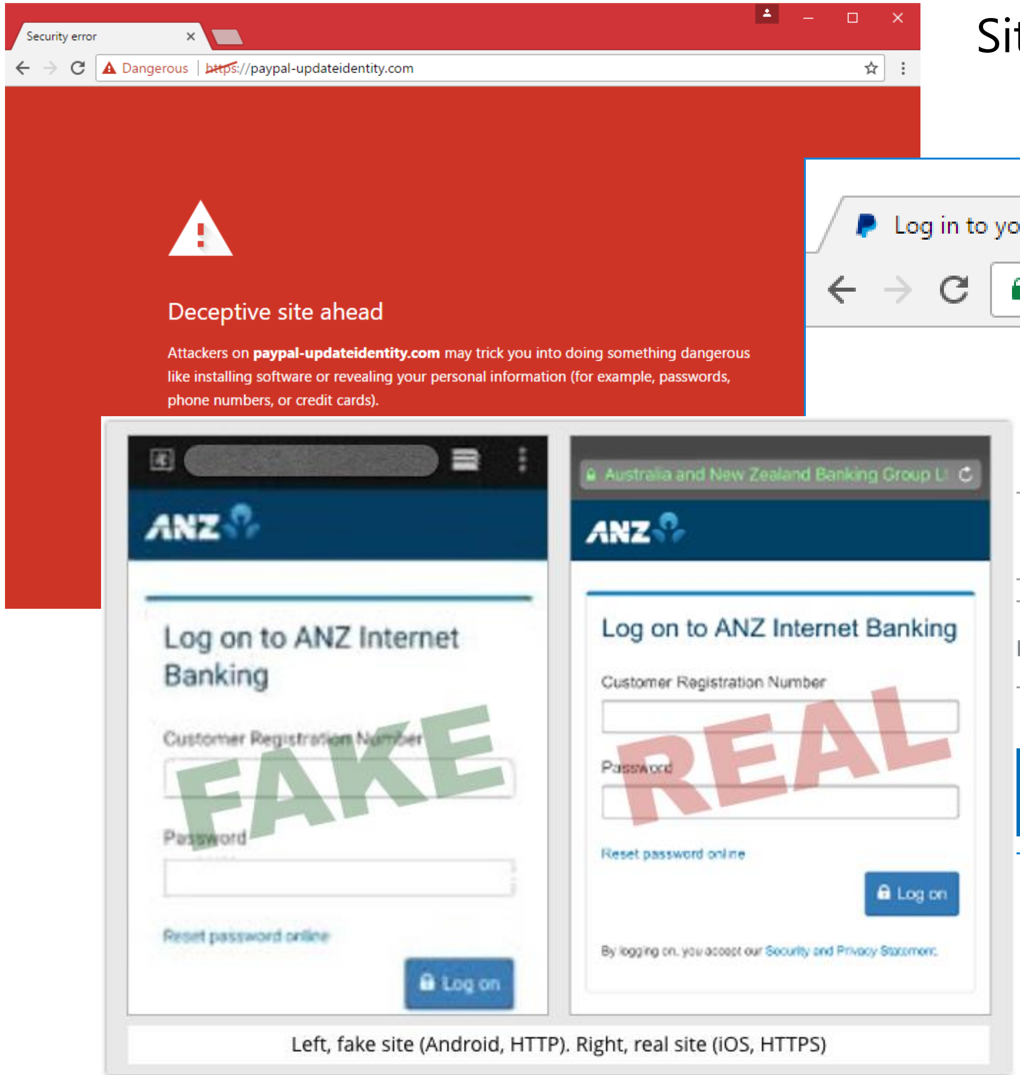
••••••••••••

https://verify-webscrid2367.serveirc.com/signin/

Phishing websites are often connected to the links found in Phishing emails. However, it is possible to stumble upon these sites through typos in the URL or malicious ads.

Double checking the web site address in the top bar will help avoid intrusions. Site will have their official domain name in the string of characters. For example the PayPal login to the left does not mention PayPal.com in the URL.

Site should always be HTTPS but you can see here that the site on the left is registered to PayPal.


Security error

Dangerous | ~~https~~://paypal-updateidentity.com

Deceptive site ahead

Attackers on **paypal-updateidentity.com** may trick you into doing something dangerous like installing software or revealing your personal information (for example, passwords, phone numbers, or credit cards).

Log on to ANZ Internet Banking

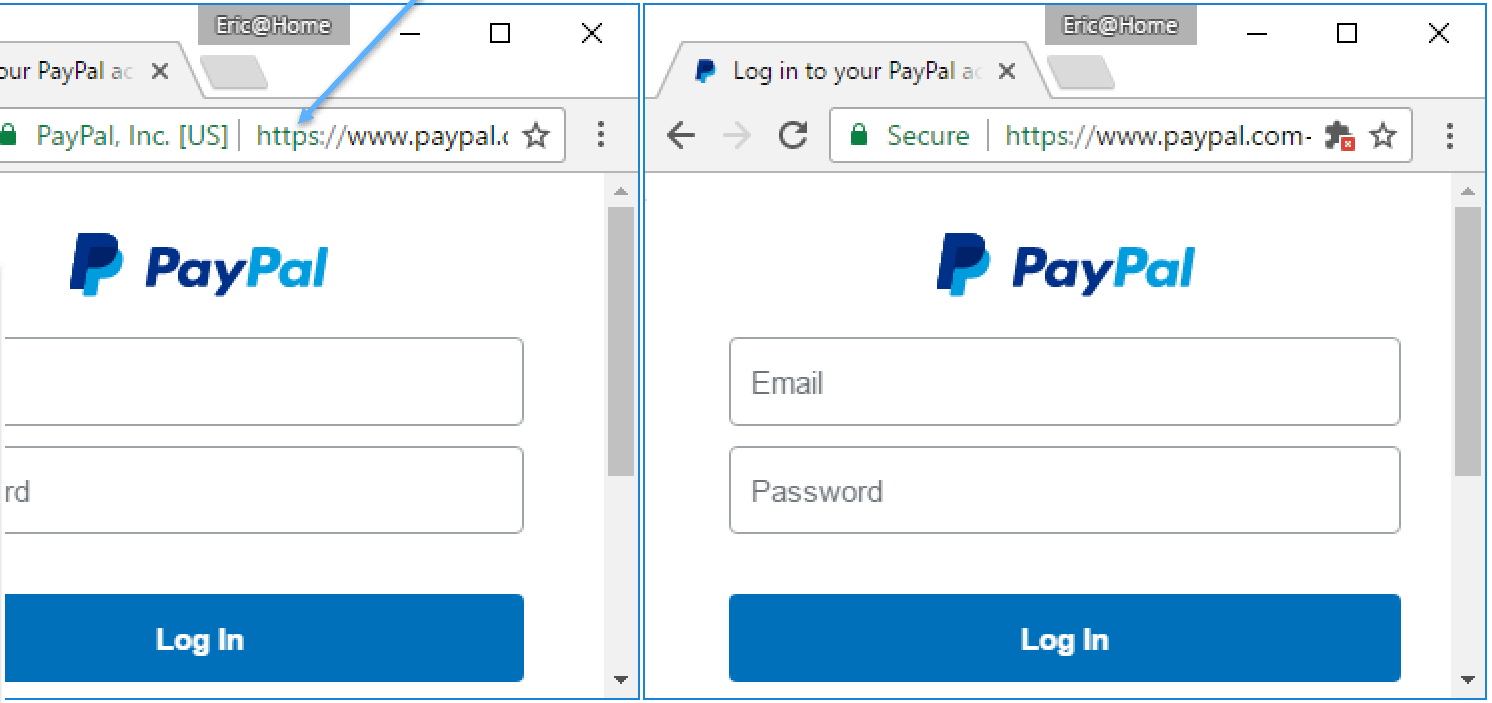
Australia and New Zealand Banking Group Li

Customer Registration Number

Password

By logging on, you accept our Security and Privacy Statement.

Left, fake site (Android, HTTP). Right, real site (iOS, HTTPS)


Log in to your PayPal ac

PayPal, Inc. [US] | https://www.paypal.c

Log in to your PayPal ac

Secure | https://www.paypal.com-

One real, one fake, your account is at stake.

If there is a logon prompt and there is no green lock in the address bar, the HTTPS has a slash through it, or it is using HTTP (missing the “S”, the site is very likely a Phishing site.

Why do users and even IT professionals fall victim?

- The attackers are organized.
- The attackers know our routines.
- The attackers know our products.
- The attackers operate much in the same way you do.

Mirazon®

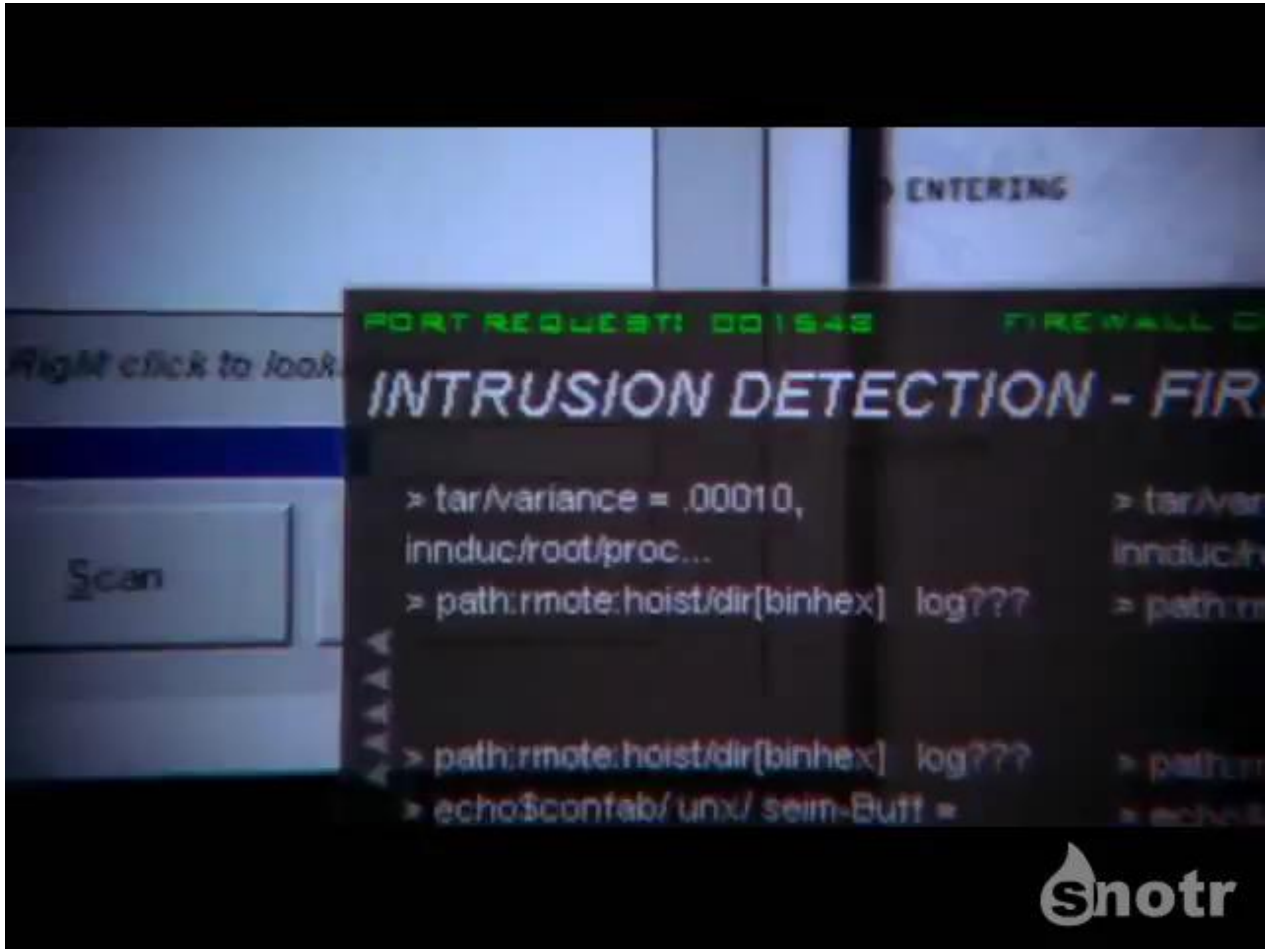
Why do users and even IT professionals fall victim?

Jim Browning 4 part scam call center full take over.
https://www.youtube.com/watch?v=le71yVPh4uk

BBC Clip covering the above.
https://youtu.be/7rmvhwwiQAY?t=215

A bit of fun. (ScamBaiters)
https://youtu.be/UmEKhOEnmpg?t=2110

What Hacking REALLY Isn’t



INTRUSION DETECTION - FIR

```
> tar/variance = .00010,
innduc/root/proc...
> path:rmote:hoist/dir[binhex]   log???

> path:rmote:hoist/dir[binhex]   log???
> echo$confab/ unx/ seim-Butt =
```

Thank you! Questions?

Rance Reinhardt

Rance.Reinhardt@Mirazon.com

502-240-0404