

# INFORMATION SECURITY AWARENESS

By  
xzahirx

What should we know?



# DISCLAIMER

The views and opinions expressed in this presentation are those of author and do not necessarily represent official policy or position of current (and former) employers of the presenter.

# Who Am I



# HELLO! I AM JUST ORDINARY PERSON...

- HND in Computing (BIT) at Kolej Profesional Mara Beranang, batch 2001
- Bachelor of Engineering Technology (Hons) in Network System at UniKL MIIT, BNS batch 2006
- Master of Science in Computer Networking at UiTM Shah Alam, CS778 batch 2012
- PhD in IT at UniKL MIIT, batch 2018
- MIMOS Berhad 2009-2010 Code 8 Apprentice
- AIG Global Services (M) 2010 Junior System Engineer
- IIUM 2010-2018 Network Engineer (J41)
- OUM Tutor and FYP Supervisor
- GFM Services Berhad 2018 IT Engineer
- Maybank 2019 Senior Network Engineer
- Celcom Axiata Berhad Information Security Solution & Engineering
- Members of:
  - OWASP (Open Web Application Security Project)
  - MGTI (Malaysia Global Threats Intelligence)
  - RawSEC Committee
  - BEM Technologist Member ID: T10213
  - MBOT Member ID: GT18080296



MOHAMMAD ZAHIR BIN  
MAT SALLEH



The leak is already under investigation in Pakistan since last month, April 2020.

By Catalin Cimpanu for Zero Day | May 6, 2020 -- 01:00 GMT (09:00 GMT+08:00) | Topic: Security



*Image: Annie Spratt*

[MORE FROM CATALIN CIMBANU](#)



**Google**  
Chrome 84 released with support for blocking notification popups on spammy sites



**Security**  
Microsoft July 2020  
Patch Tuesday fixes 123  
vulnerabilities



**Security**  
RECON bug lets hackers  
create admin accounts  
on SAP servers



**Security**  
A hacker is selling details of 142 million MGM hotel guests on the dark web

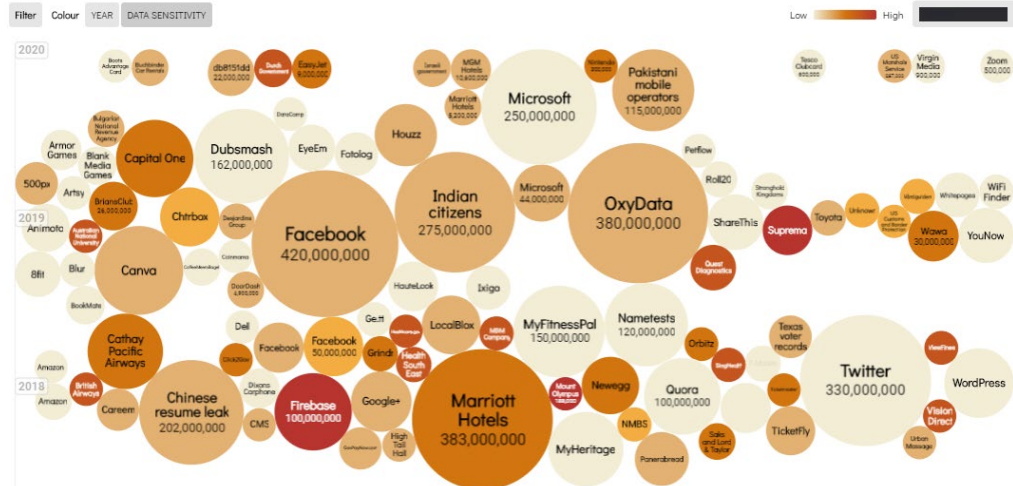
## VLJANDREN - OCTOBER 30, 2017 1.3K 15 511K READS



Telco/MVNO	Total Records	Last Updated
Celcom Prepaid	10,548,183	03-06-2014
Celcom Postpaid	4,194,315	03-06-2014
Digi Prepaid	11,411,815	30-05-2014
Digi Postpaid	2,036,730	30-05-2014
Umobile postpaid + prepaid	3,866,672	30-05-2014
Maxis Postpaid	2,840,741	29-07-2014
Maxis Hotlink	9,562,019	29-07-2014
Friendi Mobile	43,523	29-06-2014
MerchantradeAsia	446,203	07-07-2014

Select losses greater than 30,000 records  
Last updated: 11th May 2020

*Last updated: 11th May 2020*



MGM Resorts said security incident took place last summer and notified impacted

By [Catalin Cimpanu](#) for [Zero Day](#) | February 19, 2020 -- 23:27 GMT (07:27 GMT+08:00) | Topic: [Security](#)





# Impact of cyber attack

## Financial

- theft of corporate information
- theft of financial information
- theft of money
- disruption to trading
- loss of business or contract

## Reputation

- loss of customers
- loss of sales
- reduction in profits

## Legal consequences

- fines
- regulatory sanctions

# Security Matters to Everyone



Top Management

Business Owners

Employees

Third-parties  
(vendors/ contractors/ Suppliers etc)

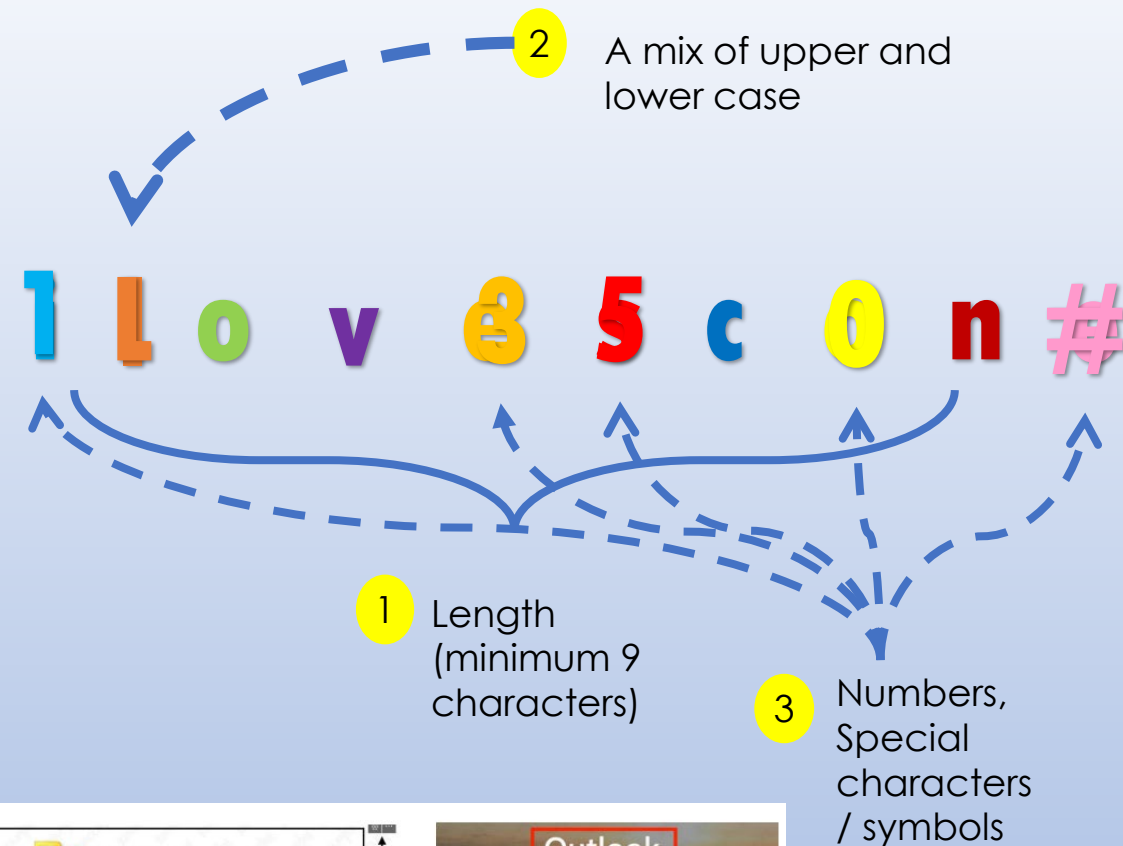
Customers



# Your Role

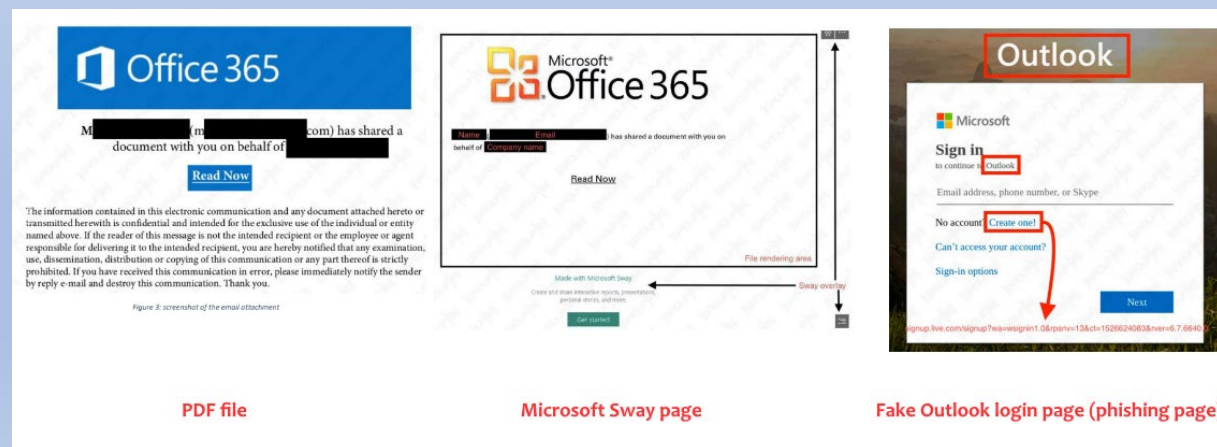
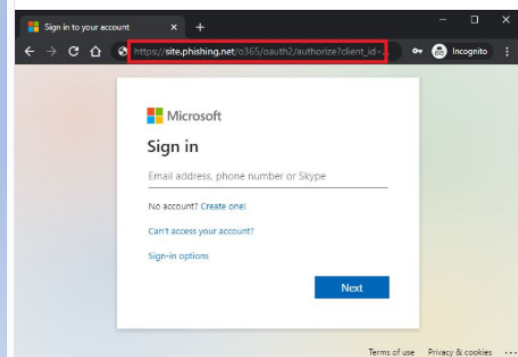
## Keep your Password safe

- Create Unique and secure password
- Change regularly at least 90 days
- Never share your password
- Turn on MFA – Microsoft Authenticator



New phishing attack targeting Microsoft Teams users aims to steal Office 365 credentials

Carefully check the URL before you login. Microsoft Office 365 legit domain used for login purposes is **microsoftonline.com**



PDF file

Microsoft Sway page

Fake Outlook login page (phishing page)



# Your Role

## Be Aware

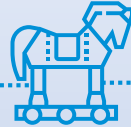


### Malware



#### WORMS

Spread automatically



#### TROJAN

Disguised as legitimate software



#### VIRUS

Spread with user action



#### SPYWARE

Monitors your activity



#### ADWARE

Maliciously feeds you ads



#### RANSOMWARE

Pay ransom money to unlock the computer



**Phishing** - A technique used to gain personal information for purpose of identity theft, using fraudulent e-mail messages that appear to come from legitimate businesses.



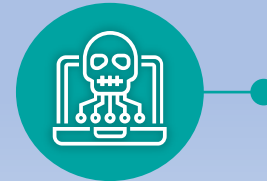
**Social Engineering** - Manipulate an individuals to give away confidential and valuable information.



**Man-in-the-middle Attack** - A type of eavesdropping attack that occurs when a malicious actor inserts himself as a relay/proxy into a communication session between people or systems.



**Brute-force Attack** - A trial-and-error method used to obtain information such as a user password or personal identification number (PIN). In a brute force attack, automated software is used to generate a large number of consecutive guesses as to the value of the desired data.



**Exploit of Unpatched Software** - An unpatched software leaves a backdoor for hackers to exploit which can put business in serious security risks.



# Best Practices for Working at Home




- ➔ **Secure your Home Network**
  - Change default administrator password
  - Allow only people you trusted
  - Make your password stronger
  
- ➔ **Keep Up-to-date**
  - Make sure each of your computers, mobile devices, programs and apps are running the latest version of its software
  - Ensure your anti-virus is the current version
  
- ➔ **Separate your work and personal devices**
  - Explains to your children, friends, or other family members that they cannot use your work devices
  - Windows lock (CTRL-ALT-DEL) before you leave your laptop unattended.

# WHATSAPP HIJACKING

<https://www.celcom.com.my/support/tips-and-tricks/2021/protecting-yourself-from-whatsapp-hijacking>

# SEE CHARGES THAT YOU DONT RECOGNIZE? HERE'S WHAT YOU CAN DO

<https://www.celcom.com.my/support/tips-and-tricks/2021/see-charges-you-dont-recognize>

Products Shop Lifestyle Support Our Network


Scam Alert  
Tuesday, 6 Apr 2021

## PROTECTING YOURSELF FROM WHATSAPP HIJACKING


WhatsApp hijacking is when scammers are using the WhatsApp re-registration process to take over your WhatsApp accounts.

### How do scammers take over your WhatsApp account?


- [Impersonating as a friend or WhatsApp Support Team](#)  
Scammers will try to request for WhatsApp registration code. They will intentionally make several failed verification attempts.
- [Accessing your voicemail account](#)  
Scammers will try to access your voicemail by guessing your password/PIN.



Impersonating as a friend  
or WhatsApp Support Team



Accessing your  
voicemail account

Products Shop Lifestyle Support Our NetworkPersonal Business About UsMy Account

Support > Tips and Tricks > SEE CHARGES YOU DONT RECOGNIZE? HERE'S WHAT YOU CAN DO

Scam Alert  
Thursday, 3 Jun 2021

## SEE CHARGES THAT YOU DONT RECOGNIZE? HERE'S WHAT YOU CAN DO

If you get charged for content-related subscription and have doubts on the charges, here's a checklist of what you can do to avoid it from reoccurring.

### Mobile malware infection

Mobile malware is a malicious software specifically designed to target mobile devices. It aims to gain access to private data, abuses subscription to content services, and sends SMS spams. Some mobile malware, like MobOk Android trojans, can automatically subscribe you to paid services, which will lead to an unexplained transaction in your bill.

How do you protect yourself from mobile malware?

- Only download and install apps from official mobile app stores such as Google Play Store, Apple App Store, Huawei App Gallery, etc.
- Install an antivirus software. Update, and perform a full scan from time to time.
- Perform a factory reset if you find that your mobile phone has already been infected with malware.

Read more about mobile malware trends and evolution: <https://securelist.com/mobile-malware-evolution-2020/101029/>

### Are you a scam victim?

Have you received and responded to a call or message recently, asking you to share a code that has been sent to you via SMS? Have you clicked on a link claiming that you've won a

# Contact Me

- **Email**

[zahir@rawsec.com](mailto:zahir@rawsec.com)

- **Linkedin**

<https://www.linkedin.com/in/mohd-zahir-mat-salleh-b83ab331>

- **Twitter**

<https://twitter.com/xxxzahirxxx>

