black hat
USA 2020
AUGUST 5-6, 2020
BRIEFINGS

Safe**M**ind

A Framework for **Evaluating** and **Patching** the Human Factor in Cybersecurity

Ron Bitton

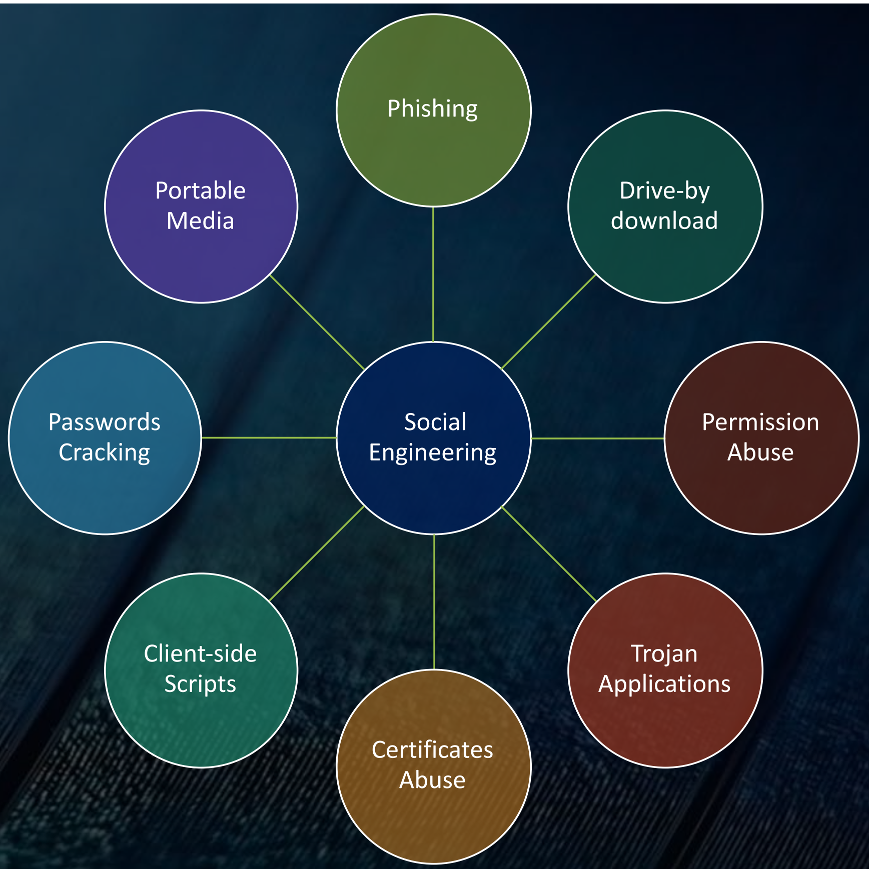
Principal Research Manager

Cyber Security Research Centre

Ben Gurion University of the Negev

1. Social engineering attacks goes **beyond phishing**

2. Social engineering attacks are **no longer limited to PCs.**



Social Engineering

Phishing

Drive-by download

Permission Abuse

Trojan Applications

Certificates Abuse

Client-side Scripts

Passwords Cracking

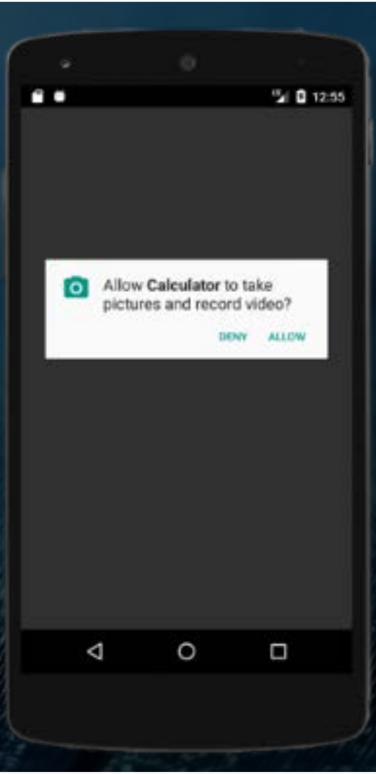
Portable Media

Social engineering attacks have changed in recent years.

1. Social engineering attacks goes **beyond phishing**

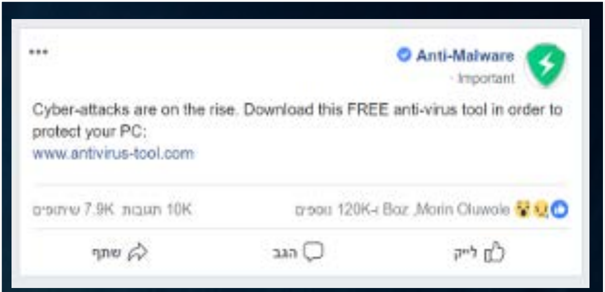
2. Social engineering attacks are **no longer limited to PCs.**

Smartphones

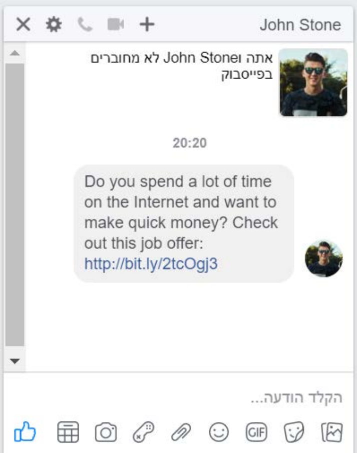


Allow **Calculator** to take pictures and record video?

Social Networks



Cyber-attacks are on the rise. Download this FREE anti-virus tool in order to protect your PC:
www.antivirus-tool.com



אתה וJohn Stone לא מחוברים בפייסבוק

20:20

Do you spend a lot of time on the Internet and want to make quick money? Check out this job offer: http://bit.ly/2tcOgj3

Social engineering attacks have changed in recent years.

1. Social engineering attacks goes **beyond phishing**

2. Social engineering attacks are **no longer limited to PCs.**

The **skills** needed by a user to mitigate different types of attacks are not the same.

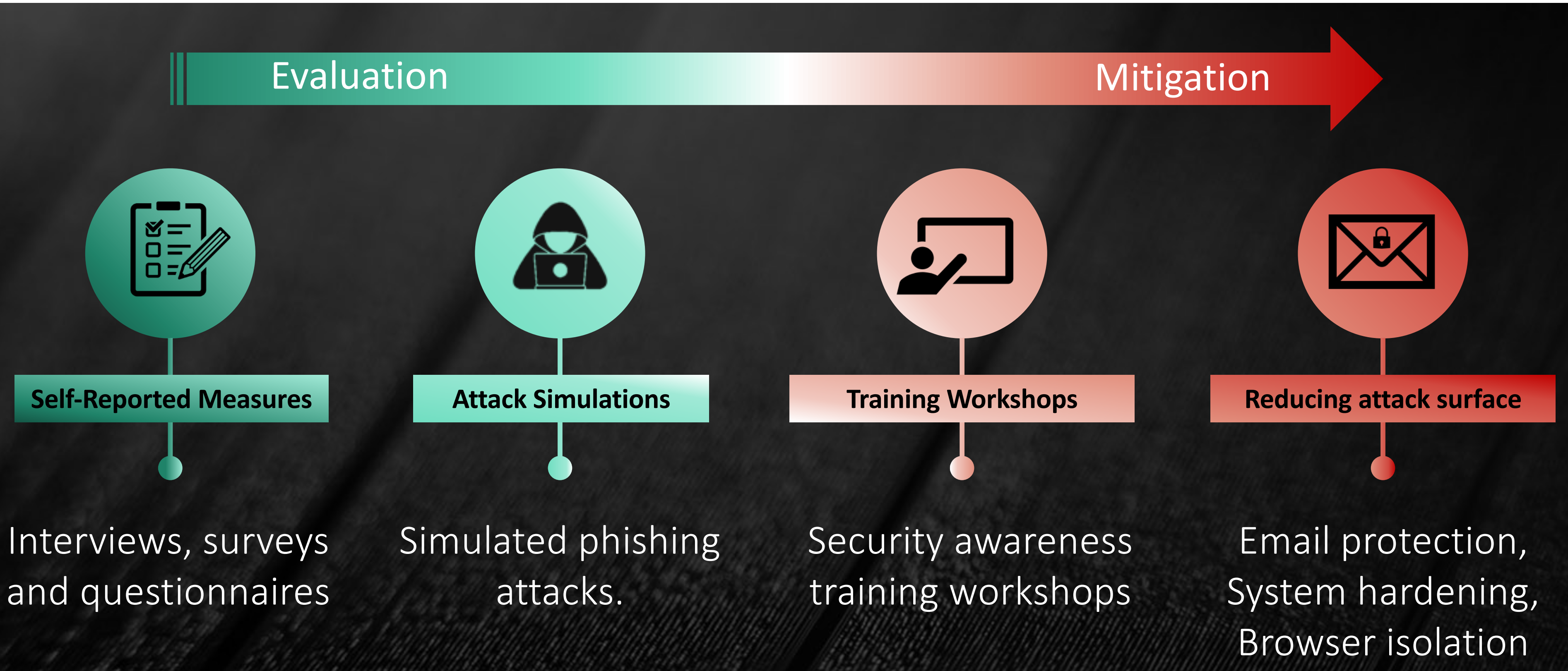
Social engineering attacks have changed in recent years.

1. Social engineering attacks goes **beyond phishing**

2. Social engineering attacks are **no longer limited to PCs.**

Despite those changes, most existing solutions **do not** distinguish between **different types of attacks and platforms.**

Social engineering attacks have changed in recent years.



Evaluation

Mitigation

Self-Reported Measures

Interviews, surveys and questionnaires

Attack Simulations

Simulated phishing attacks.

Training Workshops

Security awareness training workshops

Reducing attack surface

Email protection,
System hardening,
Browser isolation

Existing solutions for **evaluating** and **patching** the human factor in cybersecurity

- Based on self reported measures.

- Require the subjects’ active involvement and collaboration.

Interviews, surveys and questionnaires

- Based on self reported measures.

  Tend to be subjective and biased.

- Require the subjects' active involvement and collaboration.

  Consuming significant human resources and therefore are less **scalable** and cannot be performed **continuously**.

Interviews, surveys and questionnaires

- Measure the **momentary** behavior of subjects during **specific** event.

- Limited to phishing.

Attack simulations

- Measure the momentary behavior of subjects during specific event.

  Sensitive to environmental and contextual factors and therefore can be very biased.

  Cannot be used to evaluate the ISA of users continuously.

- Limited to phishing.

  Cannot be used to evaluate the ISA of users to different attack vector.

Attack simulations

- Usually performed using videos, games and posters in a controlled training environment.

Security awareness training workshops

- Usually performed using videos, games and posters in a controlled training environment.

Does not necessary reflects the behavior of users in their natural environment.

Low user engagement to the process of learning

People tend to learn the most from critiques on their own behavior, rather than generic training programs.

Security awareness training workshops

- Prevents specific exploitation techniques but leaves the vulnerability unpatched.

- Mostly limited to specific environments (e.g., a user’s working environment)

Email protection, System hardening and Browser isolation

- Prevents specific exploitation techniques but leaves the vulnerability unpatched.

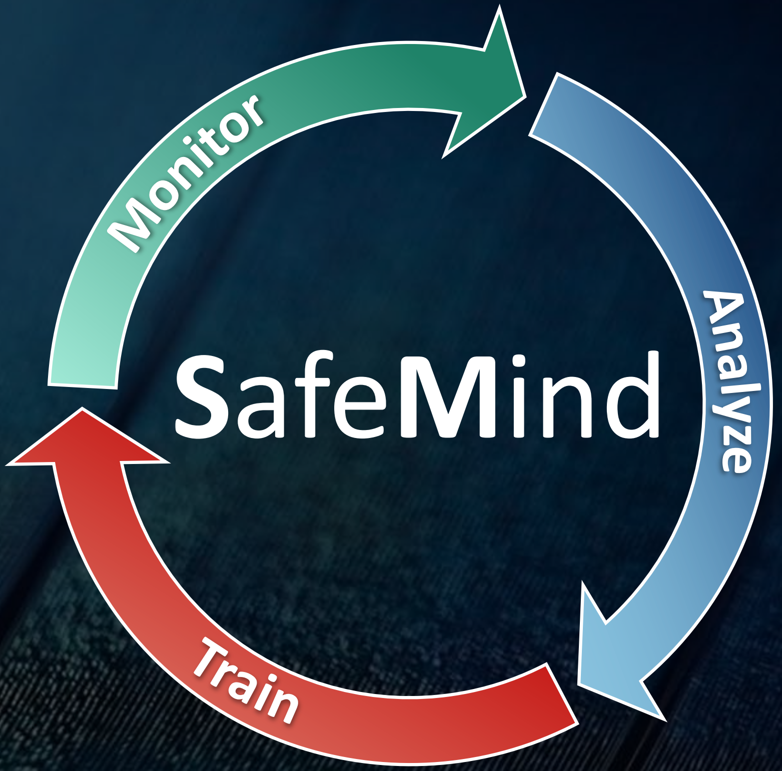
    The attacker can exploit the vulnerability using other exploitation techniques, which are not covered by the countermeasure.

- Mostly limited to specific environments (e.g., a user’s working environment)

    Cannot be used to protect the user in other environments (e.g., when working from home).

Email protection, System hardening and Browser isolation

An automated and framework for continuously and objectively evaluating the resilience of users to specific types of social engineering attacks.



SafeMind

The critical success factors in the development of SafeMind

1	**ANALYZE**	What are the **criteria** for a security aware user? What are the **importance** of different criteria in mitigating different types of attacks?
2	**MONITOR**	Given a user, how we **evaluate** those criteria **continuously**, and **objectively**?
3	**TRAIN**	Given a vulnerable user, how we **make a behavioral change** that will last long

Defining the criteria for a security aware user

01

Exploring social engineering attack case studies

02

Identifying the technologies that are compromised by the attacker

03

Enumerating the countermeasures that can be used to protect these technologies

04

Identifying the human factor vulnerabilities that are exploited by the attacker

05

Formulating the *criteria* required from a user to mitigate the attack.

The criteria for a security aware user

Application

- ✓ Download apps solely from trusted sources.
- ✓ Does not install apps that require dangerous permissions.
- ✓ Does not install apps with a low rating.
- ✓ Rarely installs apps that require root privileges.
- ✓ Regularly update apps.
- ✓ Rarely clicks on advertisements.
- ✓ Properly manages running/installed apps.
- ✓ Does not install unsinged applications

Browsing

- ✓ Does not enter malicious domains and operates in accordance with security alerts.
- ✓ Prefer to use HTTPS sites.
- ✓ Prefers to download files via HTTPS.
- ✓ Does not send sensitive information via HTTP.
- ✓ Does not insert private information into popups or advertisement cites.
- ✓ Deletes unknown certificates.
- ✓ Does not use untrusted certificates.

Virtual Communication

- ✓ Does not open emails/messages received from unknown senders
- ✓ Does not open emails classified as spam.
- ✓ Does not execute attachments received from unknown senders.
- ✓ Does not click on URL's received from unknown senders.

Virtual Accounts

- ✓ Updates passwords regularly.
- ✓ Use unguessable and diverse passwords.
- ✓ Does not store passwords unsafely.
- ✓ Uses two-factor authentication mechanisms.
- ✓ Uses password management services.

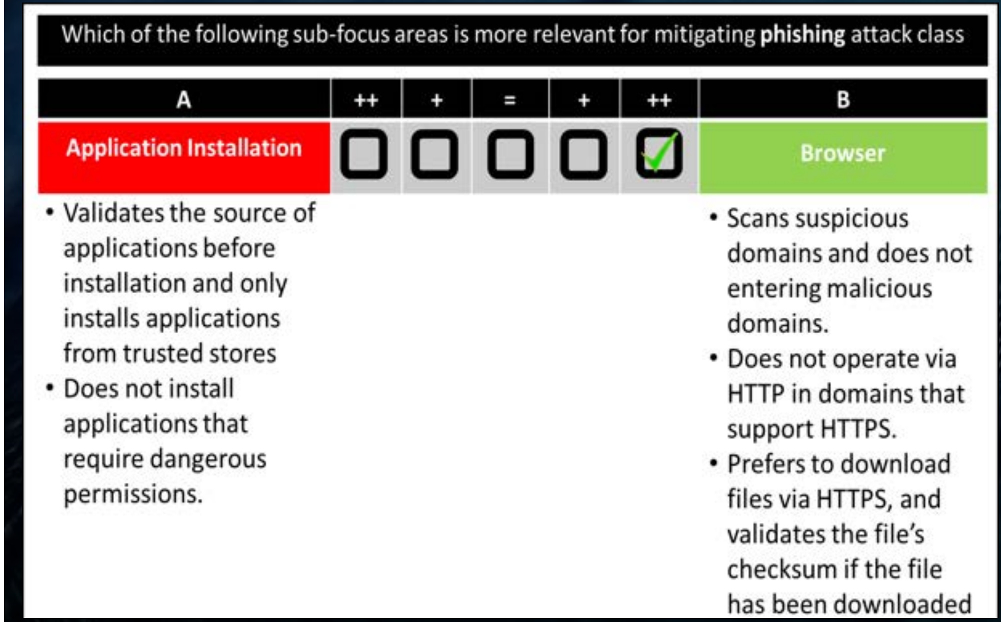
Safeguards

- ✓ Uses embedded security systems.
- ✓ Uses antivirus application.
- ✓ Updates security systems.
- ✓ Operates in accordance with security alerts (i.e., does not ignore security alerts).
- ✓ Uses PIN-code/pattern/ fingerprint.

Physical Channels

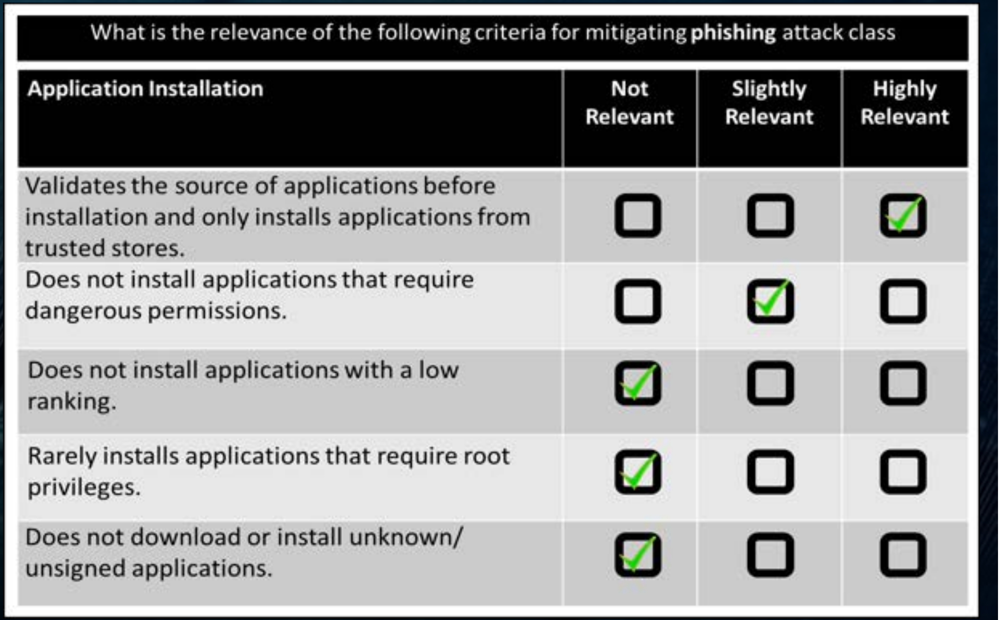
- ✓ Does not connect to unencrypted Wi-Fi networks
- ✓ Does not download files on unencrypted Wi-Fi networks.
- ✓ Uses VPN services.
- ✓ Does not transmit private data via unencrypted channels.
- ✓ Enables Bluetooth, Wi-Fi, NFC, and GPS only while they are in use.
- ✓ Connects trusted Bluetooth and NFC devices.
- ✓ Does not connect unknown media to your device.

Deriving the importance of different criteria in mitigating different types of attacks



Which of the following sub-focus areas is more relevant for mitigating **phishing** attack class

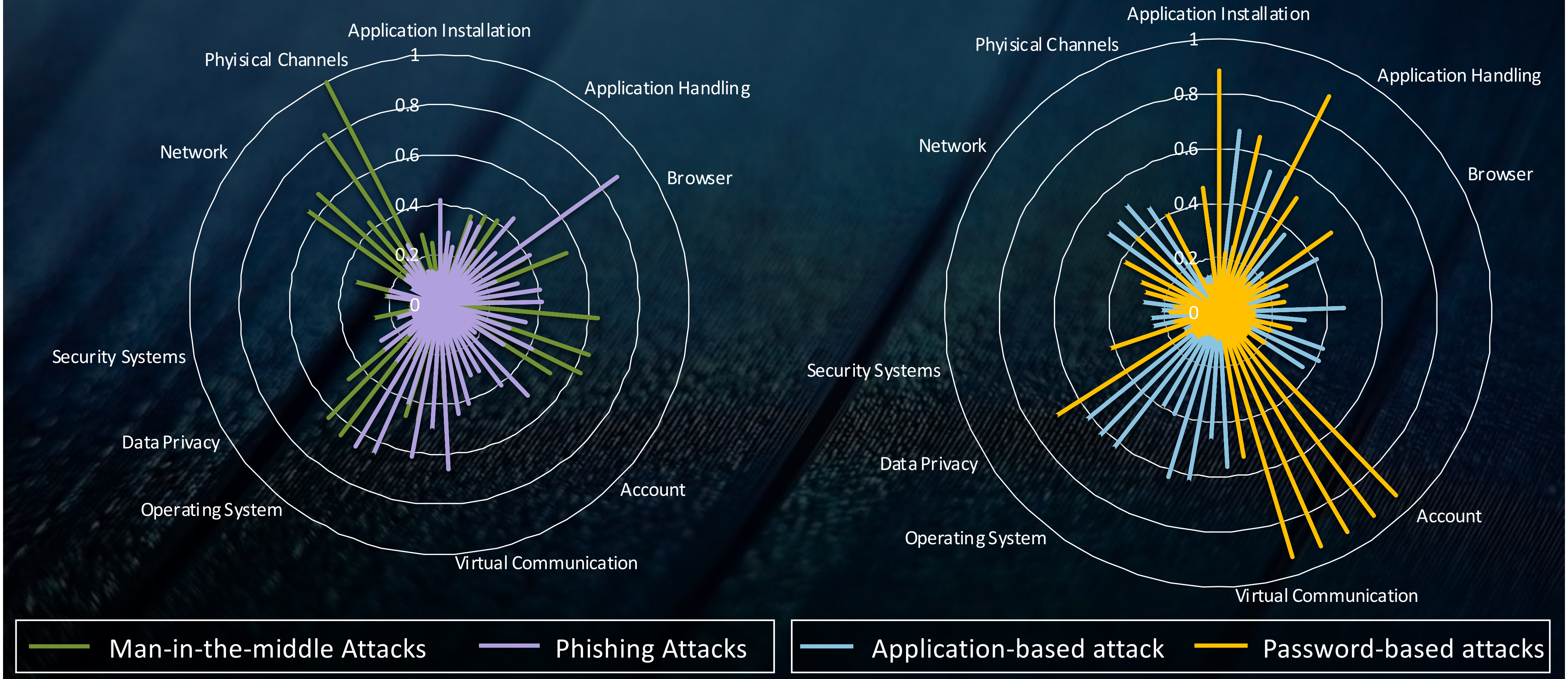
A	++	+	=	+	++	B
Application Installation	□	□	□	□	☑	Browser
• Validates the source of applications before installation and only installs applications from trusted stores • Does not install applications that require dangerous permissions.						• Scans suspicious domains and does not entering malicious domains. • Does not operate via HTTP in domains that support HTTPS. • Prefers to download files via HTTPS, and validates the file's checksum if the file has been downloaded



What is the relevance of the following criteria for mitigating **phishing** attack class

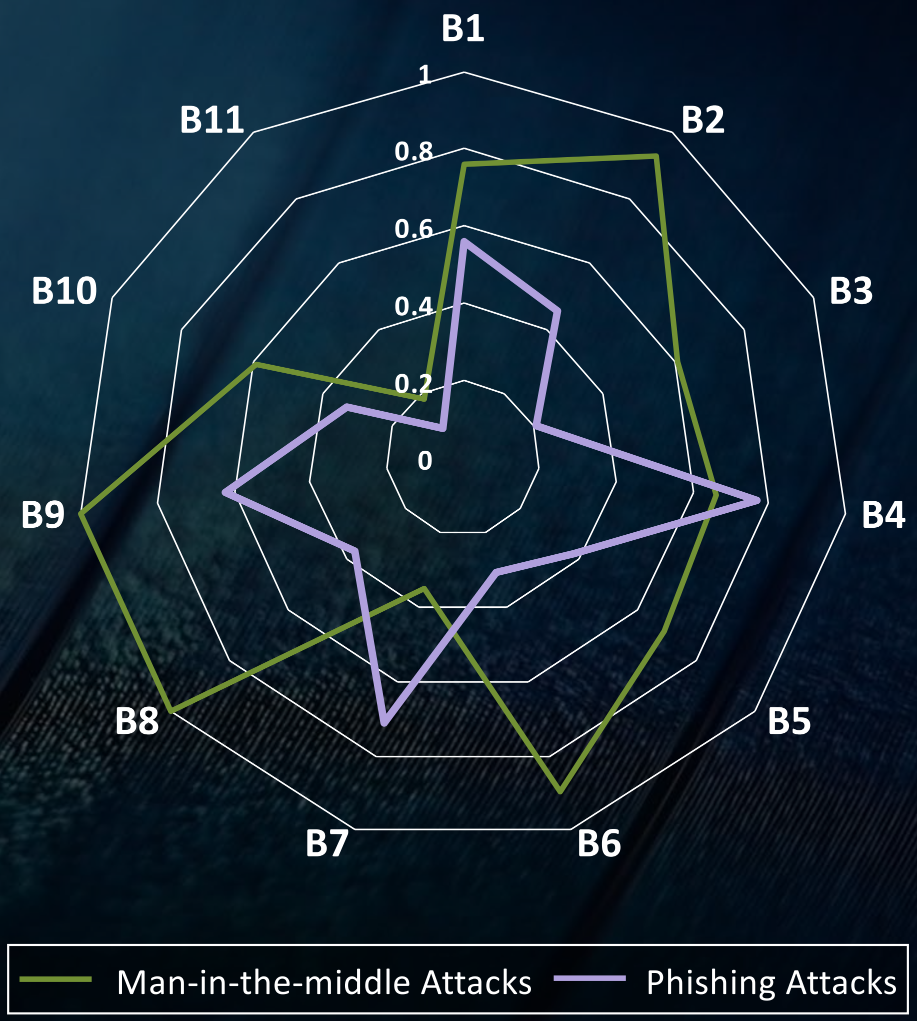
Application Installation	Not Relevant	Slightly Relevant	Highly Relevant
Validates the source of applications before installation and only installs applications from trusted stores.	□	□	☑
Does not install applications that require dangerous permissions.	□	☑	□
Does not install applications with a low ranking.	☑	□	□
Rarely installs applications that require root privileges.	☑	□	□
Does not download or install unknown/ unsigned applications.	☑	□	□

The different awareness models



Browser Technologies

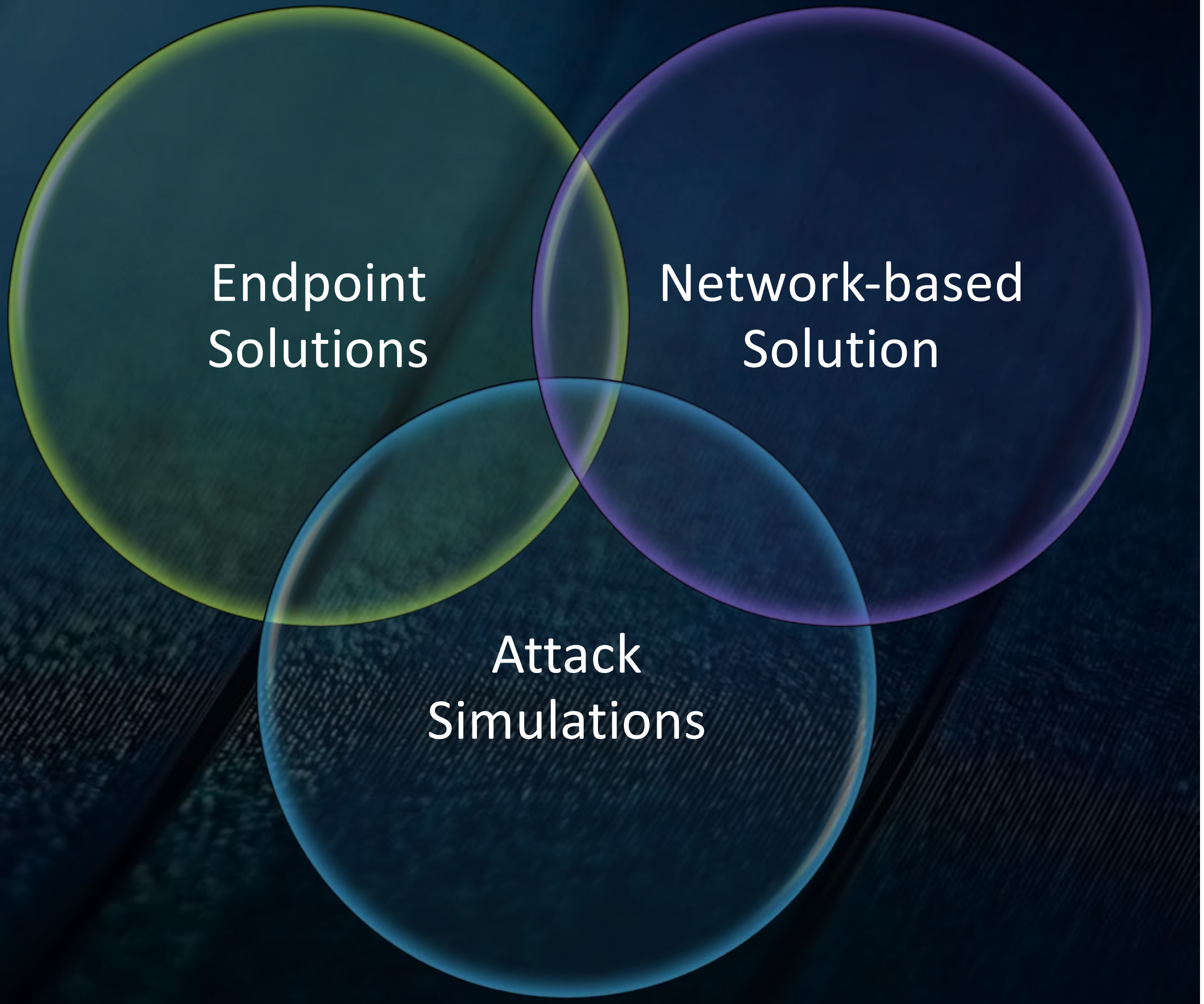
- B4 – Does not send sensitive info via HTTP
- B7 – Does not insert private info on unvalidated websites
- B6 – Deletes unknown certificates from the device
- B8 – Does not approve unknown certificates
- B9 – Does not ignore security alerts



The critical success factors in the development of SafeMind

1	ANALYZE	What are the **criteria** for a security aware user? What are the **importance** of different criteria in mitigating different types of attacks?
2	MONITOR	Given a user, how we **evaluate** those criteria **continuously**, and **objectively**?
3	TRAIN	Given a vulnerable user, how we **make a behavioral change** that will last long

Given a user how can we evaluate those criteria?

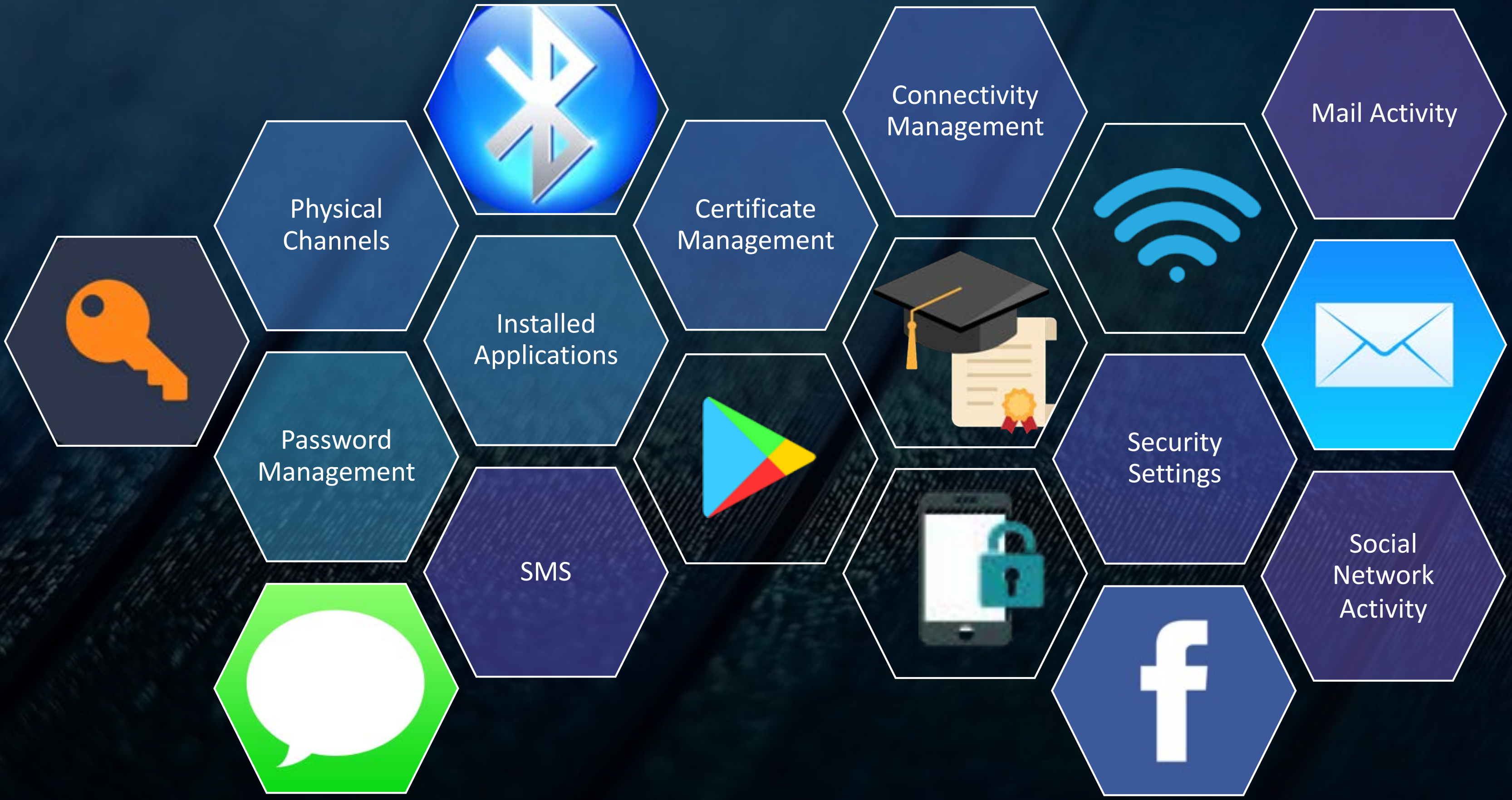


Endpoint Solutions

Network-based Solution

Attack Simulations

Information extracted using the endpoint solution



Physical Channels

Password Management

Installed Applications

SMS

Certificate Management

Connectivity Management

Security Settings

Mail Activity

Social Network Activity

Information extracted using the network solution

Application Level Protocols

- Detecting OS update version
- Certificate handling

Deep Packet Inspection

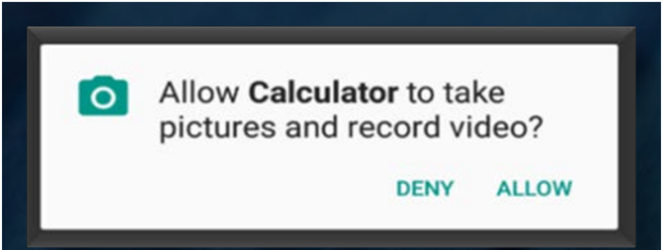
- Detecting personal information transmitted in plaintext
- Detecting unencrypted file downloads

Domain Categorization

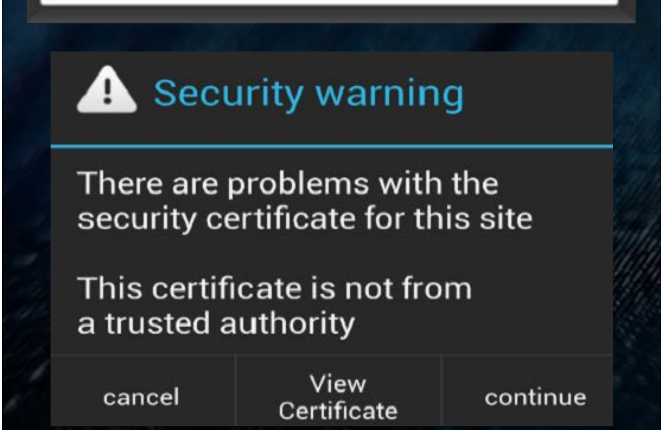
- Detecting installed applications
- Detecting malicious websites
- Detecting pop-ups and ad clicks
- Detecting uses of security countermeasures
- Detecting downloads from untrusted stores

Attack simulations

Smartphones



Allow **Calculator** to take pictures and record video?

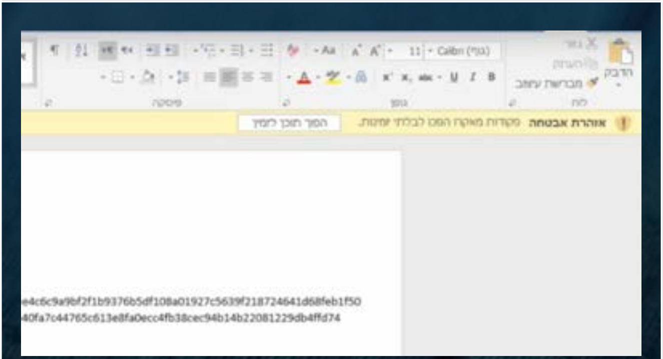


Security warning

There are problems with the security certificate for this site

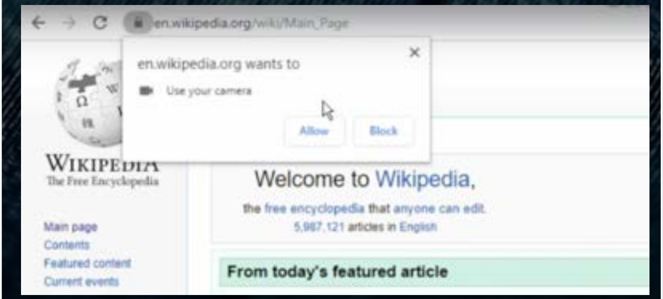
This certificate is not from a trusted authority

PC



אזהרת אבטחה פקודות מאקרו הפכו לבלתי זמינות.

```
e4c6c9a9bf2f1b9376b5df108a01927c5639f218724641d68feb1f50
40fa7c44765c613e8fa0ecc4fb38cec94b14b22081229db4ffd74
```



en.wikipedia.org wants to

Use your camera

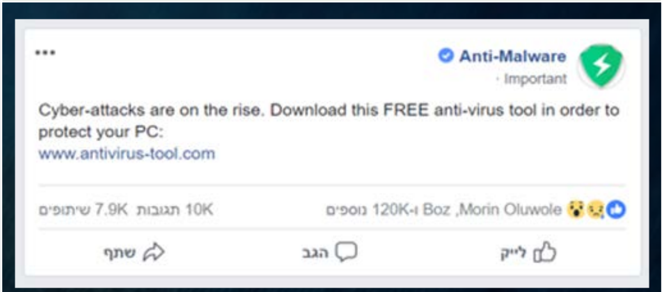
Welcome to Wikipedia,

the free encyclopedia that anyone can edit.

5,987,121 articles in English

From today's featured article

Social Networks

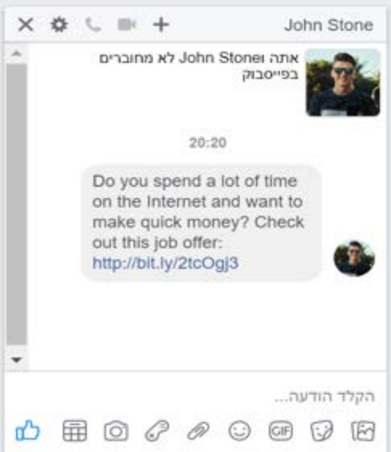


Anti-Malware
· Important

Cyber-attacks are on the rise. Download this FREE anti-virus tool in order to protect your PC:
www.antivirus-tool.com

Morin Oluwole, Boz ו-120K נוספים

10K תגובות 7.9K שיתופים

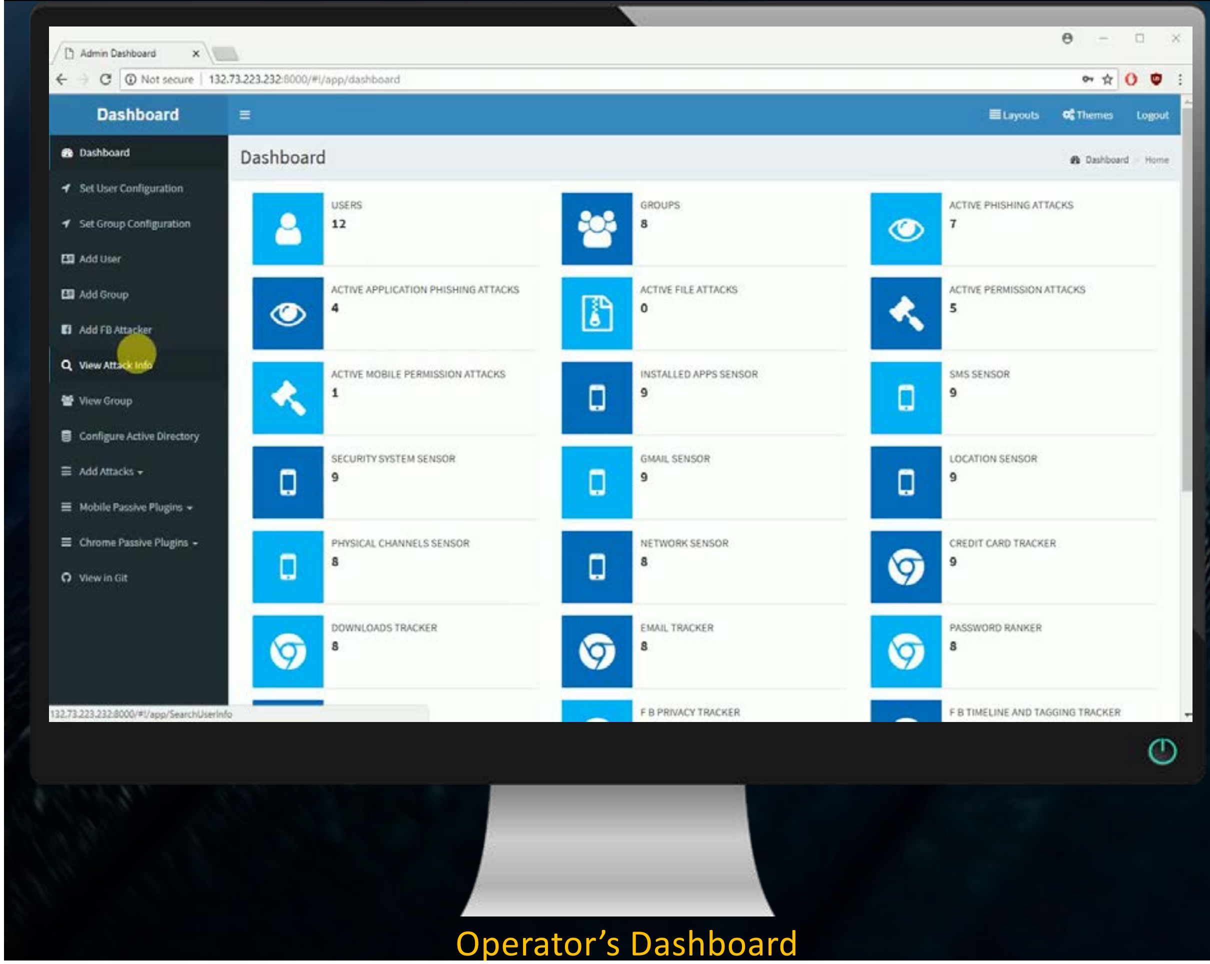


אתה וJohn Stone לא מחוברים בפייסבוק

20:20

Do you spend a lot of time on the Internet and want to make quick money? Check out this job offer:
http://bit.ly/2tcOgj3

Short Demo – Application Phishing Simulation



Dashboard

USERS
12

GROUPS
8

ACTIVE PHISHING ATTACKS
7

ACTIVE APPLICATION PHISHING ATTACKS
4

ACTIVE FILE ATTACKS
0

ACTIVE PERMISSION ATTACKS
5

ACTIVE MOBILE PERMISSION ATTACKS
1

INSTALLED APPS SENSOR
9

SMS SENSOR
9

SECURITY SYSTEM SENSOR
9

GMAIL SENSOR
9

LOCATION SENSOR
9

PHYSICAL CHANNELS SENSOR
8

NETWORK SENSOR
8

CREDIT CARD TRACKER
9

DOWNLOADS TRACKER
8

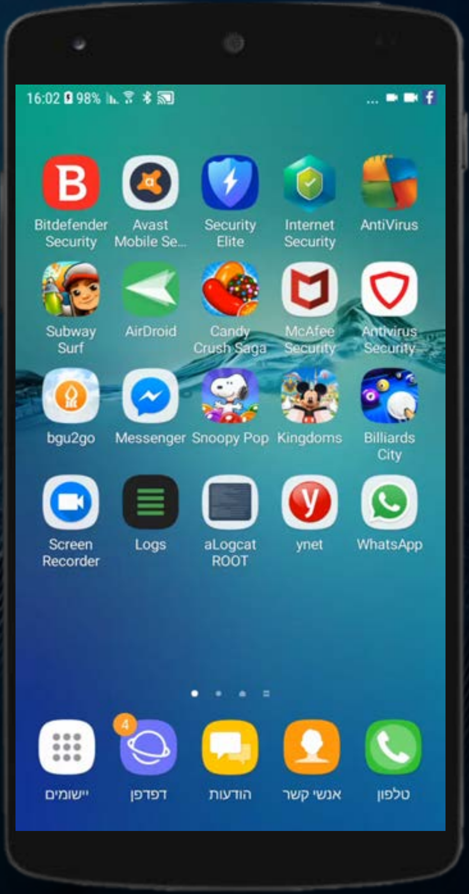
EMAIL TRACKER
8

PASSWORD RANKER
8

F B PRIVACY TRACKER

F B TIMELINE AND TAGGING TRACKER

Operator's Dashboard



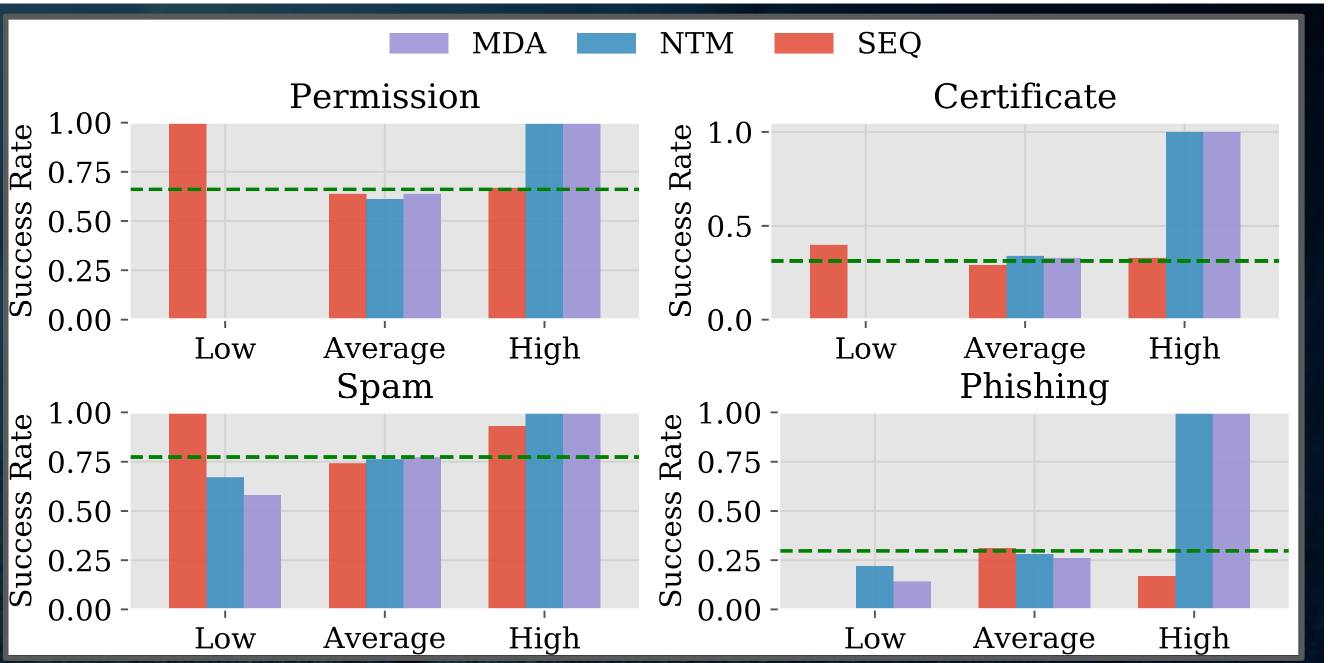
Emploee's Smartphone

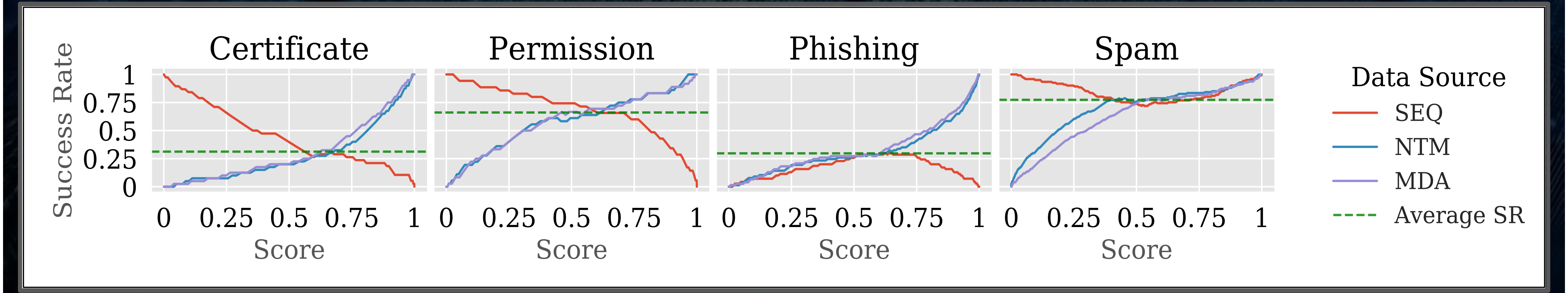
Evaluation Method

- A long-term experiment involving 162 subjects, for a duration of seven weeks.

- During the experiment we:
  - Monitored the network traffic of the subjects.
  - Measured their behavior while operating their smartphone and PC.
  - Asked them to answer the security questionnaire.
  - Exposed the subjects to four social engineering attacks.

Results


MDA
NTM
SEQ
Permission
Certificate
Spam
Phishing
Success Rate
1.00
0.75
0.50
0.25
0.00
1.0
0.5
0.0
Low
Average
High


Certificate
Permission
Phishing
Spam
Success Rate
1
0.75
0.5
0.25
0
0
0.25
0.5
0.75
1
Score
Data Source
SEQ
NTM
MDA
Average SR

Conclusions

- The self-reported behavior of subjects might **differ significantly** from their actual behavior.
- Security awareness scores derived from data collected by endpoint and network-based solutions are **highly correlated** with the users' success in mitigating social engineering attacks.

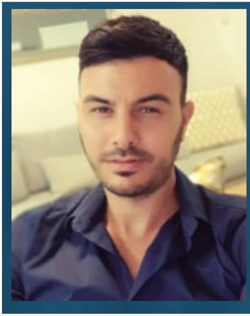
Thank you!

CBG / CSRC

Cyber@Ben-Gurion University of the Negev

Cyber Security Research Center

Israel National Cyber Bureau



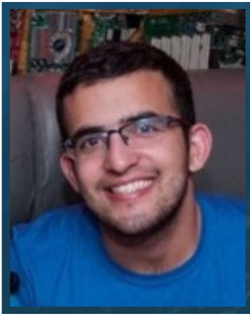
Ron Bitton

Principal Research Manager
Cyber Security Research Centre at Ben Gurion University of the Negev

This talk was partially based on the following two academic papers:

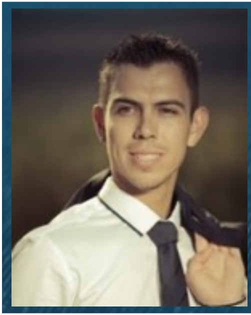
[1] Ron Bitton, Andrey Finkelshtein, Lior Sidi, Rami Puzis, Lior Rokach, Asaf Shabtai: Taxonomy of mobile users' security awareness. Computers & Security 73: 266-293 (2018).

[2] Ron Bitton, Kobi Boymgold, Rami Puzis, Asaf Shabtai: Evaluating the Information Security Awareness of Smartphone Users. 2020 CHI Conference on Human Factors in Computing Systems.



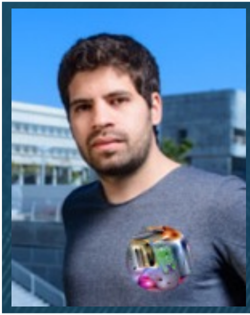
Kobi Boymgold

Security Researcher
Cyber Security Research Centre at Ben Gurion University of the Negev



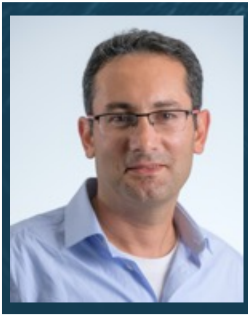
Andrey Finkelsthein

Data Scientist & Security Researcher at IBM



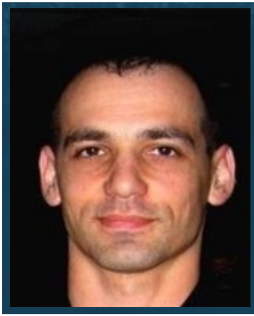
Lior Sidi

Data Scientist & Machine Learning Entrepreneur
Cyber Security Research Centre at Ben Gurion University of the Negev



Asaf Shabtai

Associate Professor
Cyber Security Research Centre at Ben Gurion University of the Negev



Rami Puzis

Assistant Professor
Cyber Security Research Centre at Ben Gurion University of the Negev

Lior Rokach

Full Professor
Cyber Security Research Centre at Ben Gurion University of the Negev