Prevenire il Furto di Identitá Online

Webinar 25 marzo 2021

Dr. Alessandro Parisi

Parte I: Comprendere il problema

Dispersione dei dati personali online

Innovation exploited

Come nella favola di Pollicino, lasciamo le tracce nella rete come molliche di pane, soltanto che queste non sono “biodegradabili”, ma persistono nel tempo

Dispersione dei dati personali online

Innovation exploited

Come nella favola di Pollicino, lasciamo le tracce nella rete come molliche di pane, soltanto che queste non sono “biodegradabili”, ma persistono nel tempo

l’uso dei Big Data Analytics consente alle aziende Tech di mettere a sistema i dati frammentati e dispersi, disponibili sulla rete

Dati comuni e furto di identità

Anche i dati personali “comuni” sono meritevoli di protezione: essi sono ad es. sufficienti per realizzare truffe o falsificare documenti

Dati comuni e furto di identità

Anche i dati personali “comuni” sono meritevoli di protezione: essi sono ad es. sufficienti per realizzare truffe o falsificare documenti

Non ho nulla da nascondere ma tutto da proteggere!

Collasso del contesto

Non sappiamo chi potrà utilizzare i nostri dati **decontestualizzandoli**

Collasso del contesto

Non sappiamo chi potrà utilizzare i nostri dati **decontestualizzandoli**

es. foto del ricoverato in ospedale, utilizzate per realizzare truffe sentimentali

Utilizzo di immagini di terzi ignari

Nessi di causalità lineari

incapacità di mettere in relazione tra loro eventi accaduti in tempi e luoghi differenti, a causa dell'apparato percettivo evolutosi nel "mediocristan", dominato da relazioni **causa-effetto lineari e dirette**

Nessi di causalità lineari

incapacità di mettere in relazione tra loro eventi accaduti in tempi e luoghi differenti, a causa dell'apparato percettivo evolutosi nel "mediocristan", dominato da relazioni **causa-effetto lineari e dirette**

es. data breach i cui effetti negativi si sviluppano a distanza di tempo, e in luoghi virtuali differenti e imprevedibili

Data breach home banking

Ubiquità dell’identità digitale

essere in posti virtuali diversi nello stesso tempo ci impedisce di intuire le implicazioni reciproche tra comportamenti tenuti online nello stesso tempo

Ubiquità dell'identità digitale

essere in posti virtuali diversi nello stesso tempo ci impedisce di intuire le implicazioni reciproche tra comportamenti tenuti online nello stesso tempo

es. navigo su siti maliziosi e contemporaneamente sull'home banking, e non mi avvedo che utilizzando lo stesso device, posso condividere involontariamente info sensibili (mediante malware come keylogger, ma anche con cookie di terze parti)

Multidimensionalità del cyberspace

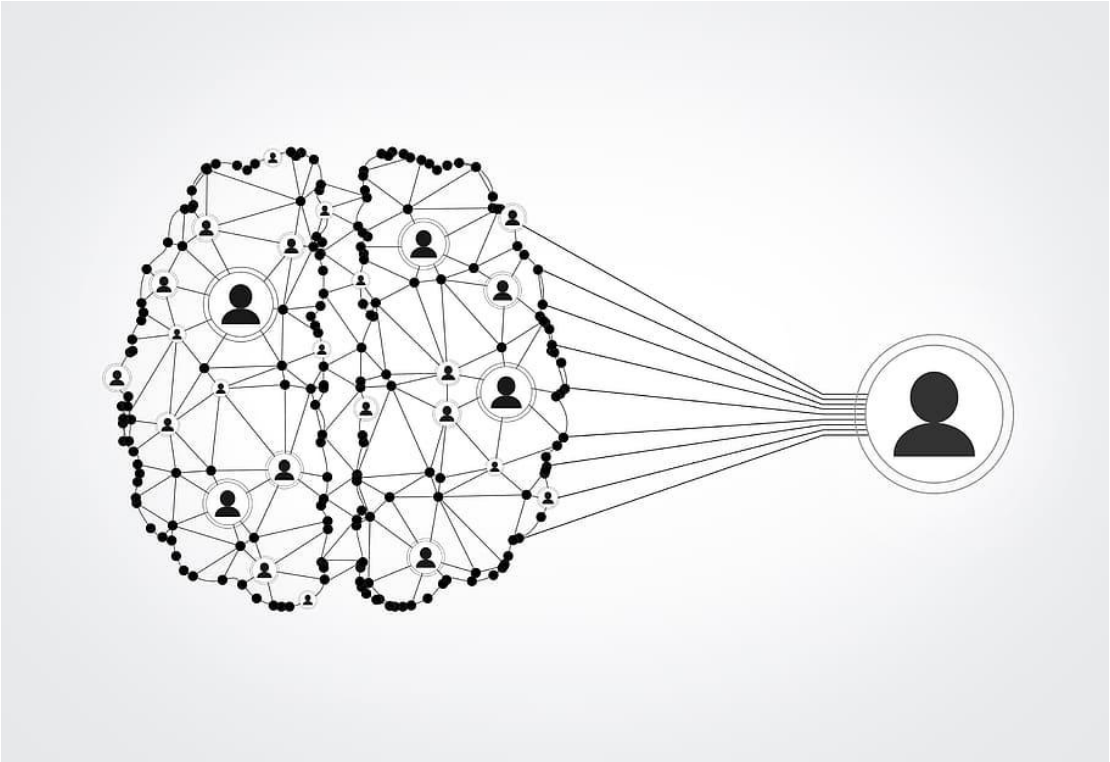
l’intuizione del ns apparato percettivo riconduce le ns. interazioni online alle consuete 3 dimensioni, e ci impedisce di valutare efficacemente i rischi associati alla complessità della rete di relazioni potenziali (paradigma IoT)

Multidimensionalità del cyberspace

l'intuizione del ns apparato percettivo riconduce le ns. interazioni online alle consuete 3 dimensioni, e ci impedisce di valutare efficacemente i rischi associati alla complessità della rete di relazioni potenziali (paradigma IoT)

CONNESSI = VULNERABILI

Multidimensionalità del cyberspace



DeepFakes, nuova frontiera del furto di identità

DeepFakes dal passato…

Parte II: Un caso concreto di furto di identità

La Kill Chain

l’attaccante deve porre in essere una serie di steps propedeutici per realizzare il suo attacco

Asimmetria informativa

Solo l’attaccante sa dove, come e quando attaccherà, difendersi da tutto significa non difendersi da nulla;

Asimmetria informativa

Solo l’attaccante sa dove, come e quando attaccherà, difendersi da tutto significa non difendersi da nulla;

assumere un atteggiamento critico per difendersi dalle minacce: è sufficiente mandare fuori bersaglio anche uno solo degli step della kill chain per neutralizzare l’attacco
Per cui attiviamo il cervello oltre che firewall e antivirus!

Le fasi iniziali del furto di identità

l’attaccante fa Osint e ricava il ns. email account, mobile number, sa che siamo correntisti della banca PincoPallo e che usiamo la app di home banking, perchè magari ci siamo lamentati dei disservizi sui social…

Predisporre l’esca per la vittima

l’attaccante ci invia una email con indirizzo mittente spoofato, spacciandosi per la banca, in cui ci invita a verificare che il ns home banking non sia stato compromesso

Predisporre l’esca per la vittima

l’attaccante ci invia una email con indirizzo mittente spoofato, spacciandosi per la banca, in cui ci invita a verificare che il ns home banking non sia stato compromesso

a tal fine, ci invita a inserire le ns credenziali di accesso senza indugio, utilizzando il link (che risulterà contraffatto) all’interno della email/sms

ID Spoofing

lo stesso sollecito via email e sms spoofato: è molto semplice realizzare l'email e l'sms spoofing, spacciandosi per la banca;

ID Spoofing


Carrier
2:22 AM
iSpoof v2.0
Number To Call:
888-555-5512
Your Spoofed Caller ID:
666-666-6666
Voice Change and Recording:
Normal
Man
Woman
Do Not Record
Record
OFF
Straight To Voicemail
Place Call
Free 2 Minute Call Mode
Call
Call History
Purchase
Settings

Phishing & Smishing

il link ci conduce ad un sito clone della banca, controllato dall'attaccante, che contiene una pagina per l'inserimento delle ns credenziali, e che ci tranquillizza, dicendo che le credenziali non sono compromesse

Phishing & Smishing

Sim swap

a questo punto, l’attaccante che ha a sua disposizione le ns credenziale, può ottenere la OTP key mediante il sim - swap

Sim swap


EUROPOL
SIM SWAPPING – A MOBILE PHONE SCAM
SIM swapping occurs when a fraudster, using social engineering techniques, takes control over your mobile phone SIM card using your stolen personal data.
HOW DOES IT WORK?
A fraudster obtains the victim's personal data through e.g. data breaches, phishing, social media searches, malicious apps, online shopping, malware, etc.
With this information, the fraudster dupes the mobile phone operator into porting the victim's mobile number to a SIM in his possession
The fraudster can now receive incoming calls and text messages, including access to the victim's online banking
The victim will notice the mobile phone lost service, and eventually will discover they cannot login to their bank account

Parte III: Misure di sicurezza

Non agire di impulso

non farsi prendere dalla fretta, indotta ad arte dall'attaccante, nel timore che le ns credenziali sono state compromesse: anzichè utilizzare il link allegato alla email/sms, aprire il browser e digitare autonomamente l'indirizzo dell'home banking: questa semplice precauzione, manda fuori bersaglio l'attacco;

Non spegnere il cervello!

è importante quindi mantenere un **atteggiamento critico** rispetto alle comunicazioni che ci vengono inviate, evitando di eseguire passivamente e meccanicanente le istruzioni che ci vengono suggerite di eseguire, specie se sotto la pressione di possibili **conseguenze negative** in caso di mancato adempimento (es. perdita del rimborso, possibilità di compromissione)

Pensare come l’attaccante

mettersi nei panni dell’attaccante e assumere un atteggiamento sospettoso: dietro un account social, anche se apparentemente riferito a persone che conosciamo nel mondo reale, può nascondersi chiunque, o l’account può essere compromesso

Pensare come l’attaccante

mettersi nei panni dell’attaccante e assumere un atteggiamento sospettoso: dietro un account social, anche se apparentemente riferito a persone che conosciamo nel mondo reale, può nascondersi chiunque, o l’account può essere compromesso

non confondiamo la foto del profilo con il volto che ci è noto: solo nel mondo reale siamo in grado di riconoscere gli amici guardandoli in faccia;

Non accettare doni dagli sconosciuti

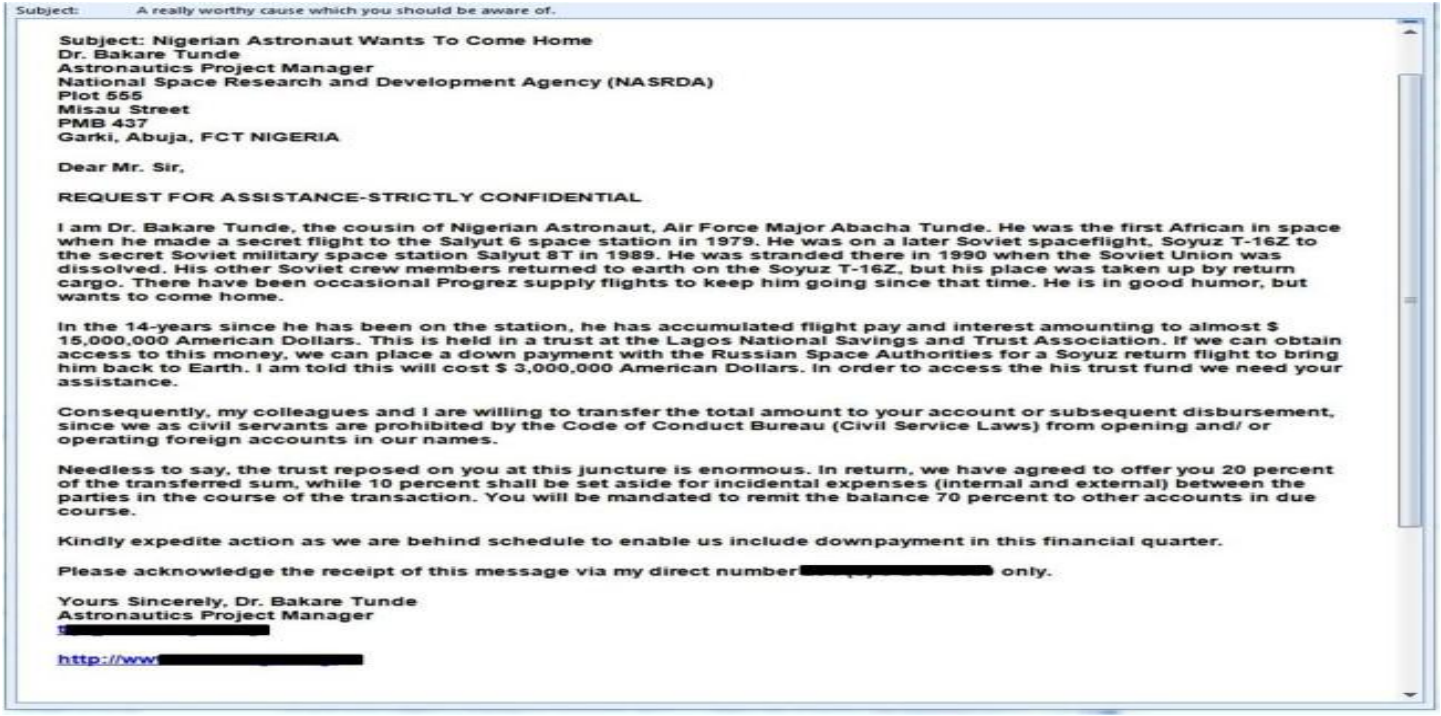
troppo bello per essere vero? Allora è certamente falso (es. dell'eredità dello zio d'America - Nigerian scam): nessuno ci fa regali / non accettare caramelle dagli sconosciuti:

Non accettare doni dagli sconosciuti

troppo bello per essere vero? Allora è certamente falso (es. dell'eredità dello zio d'America - Nigerian scam): nessuno ci fa regali / non accettare caramelle dagli sconosciuti:

ci possono carpire il ns conto corrente anche indirettamente, con la ns complicità, inducendoci a comportamenti concludenti come quello di far transitare "l'eredità" sul ns conto corrente, con la promessa di percentuali sulla stessa

Nigerian scam



Subject: A really worthy cause which you should be aware of.

Subject: Nigerian Astronaut Wants To Come Home
Dr. Bakare Tunde
Astronautics Project Manager
National Space Research and Development Agency (NASRDA)
Plot 555
Misau Street
PMB 437
Garki, Abuja, FCT NIGERIA

Dear Mr. Sir,

REQUEST FOR ASSISTANCE-STRICTLY CONFIDENTIAL

I am Dr. Bakare Tunde, the cousin of Nigerian Astronaut, Air Force Major Abacha Tunde. He was the first African in space when he made a secret flight to the Salyut 6 space station in 1979. He was on a later Soviet spaceflight, Soyuz T-16Z to the secret Soviet military space station Salyut 8T in 1989. He was stranded there in 1990 when the Soviet Union was dissolved. His other Soviet crew members returned to earth on the Soyuz T-16Z, but his place was taken up by return cargo. There have been occasional Progrez supply flights to keep him going since that time. He is in good humor, but wants to come home.

In the 14-years since he has been on the station, he has accumulated flight pay and interest amounting to almost $ 15,000,000 American Dollars. This is held in a trust at the Lagos National Savings and Trust Association. If we can obtain access to this money, we can place a down payment with the Russian Space Authorities for a Soyuz return flight to bring him back to Earth. I am told this will cost $ 3,000,000 American Dollars. In order to access the his trust fund we need your assistance.

Consequently, my colleagues and I are willing to transfer the total amount to your account or subsequent disbursement, since we as civil servants are prohibited by the Code of Conduct Bureau (Civil Service Laws) from opening and/ or operating foreign accounts in our names.

Needless to say, the trust reposed on you at this juncture is enormous. In return, we have agreed to offer you 20 percent of the transferred sum, while 10 percent shall be set aside for incidental expenses (internal and external) between the parties in the course of the transaction. You will be mandated to remit the balance 70 percent to other accounts in due course.

Kindly expedite action as we are behind schedule to enable us include downpayment in this financial quarter.

Please acknowledge the receipt of this message via my direct number [redacted] only.

Yours Sincerely, Dr. Bakare Tunde
Astronautics Project Manager
[redacted]

http://ww[redacted]

Per saperne di più

Visita il nostro sito