Being the Lecture delivered Ayobami Rotimi Mark on Iwoland Development Coalition’s WhatsApp page on Saturday, 14th of October, 2017 INFOSEC AND CYBER SECURITY.

Mr Rotimi Ayobami (CISSP, COMPTIA A+, CPT (Certified Pen Tester), CompTIA Linux+, CEH and COMPTIA SECURITY) is an IT Expert with MOYADEX GLOBAL RESOURCES.

What is Infosec

InfoSec is a short term for Information Security, and it is the practice of preventing unauthorized access, use, disclosure, destruction, modification, recording of information, either in electronic form or physical form.

The very mind of all Ethical Hacker is CIA.

What is CIA?

CONFIDENTIALITY

INTEGRITY

AVAILABILITY.

Our aim is to ensure neither of the three is compromised.

Confidentiality: is the data not disclosed

Integrity: is the data not modified or manipulated.

Availability: is the data available for proper use.

What is Cyber Security

Cyber security, also known as Computer security or IT security, and we can conclude that it is the protection of computer systems from the theft and damage to their hardware , software or information in a network, as well as from disruption or misdirection of their functions.

One can actually perceive Information Security is like a child to Cyber Security. The two are mostly used separately, as the Cyber Security itself is very wide, and on the other hand, the very goal of Computer security lies around Data/Information protection. But when you say Cyber Security, then, I can assume you are referring to varieties of ways to secure Computer System which involves the knowledge of Social engineering, Reverse engineering, Pentesting, Network monitoring, Data management, Cryptography, Web applications analysis, Password Cracking and so on,and they are all pointing to Data/Information theft/Security.

The Scope Of This lecture

Well, I'm not assuring anyone that this lecture is all you need to secure your network, either Intranet or Internet, but it should give you basic knowledge.

I can assure you that this lecture will covered all you need to know as an end user, to secure your Smartphones and Computer (PC).

Requiring more than this, simply means you will have to take one or two courses in Cyber Security depending on what it's required for.

WHAT WILL BE COVERED?

1. Social engineering

2. Securing Smartphones and PCs

Why Social Engineering?

1. Bypassing Physical Security e.g. Security door, Security men.

2. When technology can't solve the problem.

3. Post Exploitation: getting information before exploiting target.

4. Binary Evasion: when an attacker have to pass through binary system .

Psychology of Social Engineering.

1. Elicitation

2. Framing

3. Pretexting

4. Cold Calling

Social Engineer Techniques.

1. Dumpster diving

2. Impersonating

3. Shoulder surfing

4. Phishing

   I Spear-Phishing

   II Whaling.

5. Baiting

6. Interactive Voice Response (IVR)

7. Quid pro quo

8. Tailgating.

All names I will be using in this lecture is only for education purpose.

1. Elicitation

You come home and you find broken glass on the floor in your sitting room where there is three Children staring at you expecting an action.

Who did this?, You asked.

No one is ready to give you the needed information and you want to know who broke the glass.

That's where Elicitation comes in, trying to get the needed information without directly asking for the Info.

Father: CS ,Daddy Ibrahim asked me to come and see him, and I told him before I left to help me monitor you guys. Did your brothers went out?

CS: Yes, but I told them not to.

Father: what of you?

CS: No o!

Father: CS, when did they left the house?

CS: some minutes after you left.

Father: when did they return?

CS: not quite long.

Father: they returned at the same time?

CS: Yes.

Father: are you sure you didn't go out?

CS: I'm here reading.

Father: Did I have visitor?

CS: No!

Father: And you said you didn't know who broke the glass? You broke the glass.

(Daddy Ibrahim is used to convince CS, just imagining CS running out of the room to see DADDY IBRAHIM in other to confirm if He called his Dad. He will manipulate his father instead)

Do make sure you are checking the authenticity of every Information from reliable or official source , especially when it requires your personal/Private/secret Data

This is usually use to get password. Social Engineers will try all means to get your personal information e.g names,DOB, Spouse name and his/her DOB, Children names and their DOB, Pets, Favourite Colour, Favourite Music and so on. Why do Social Engineers need those information? It's used to crack password. 80% made their passwords up from the informations. CRUNCH is a very powerful password cracking tools, you will pass the victim information and the target website's login page to it, then it will try all possible combinations against the target website, and it's 💯 sure CRUNCH will crack your password assuming it's from the Information given to it, no matter the combination. The remaining problem lies on the target website's login authentication.

2. Framing

Framing is actually when I set up a Topic of discussion and frame my questions around it. In this type of attack, the Social Engineer always drive the topic, as he will direct the conversation to the direction he chooses to get all needed information. It's similar to Elicitation.

Example: I want to impersonate someone to a bank as Supervisor. So I need some information, I'm going to target someone in the bank to get necessary informations which is going to be Mr Jubreal Akintayo.

Rotimi: Hello Big brother

Akintayo: Yeah.

Rotimi: how are you doing Sir?

Akintayo: Great! Do I know you?

Rotimi: haaaaaaa, 😂. You don't recognise me again. Well, I will come home soon.

When I get to you, you will have to do this▯ ♂ forgetting one of your little brother.

Akintayo: OK!

Rotimi: the issue is, I was employed to Dazuki bank, and we are asked to come for seminar or whatever tomorrow.

Akintayo: congrats.

Rotimi: So I remember I have a brother in Iwo, that is also working in Dazuki bank.

Akintayo: OK

Rotimi: So, I want you to advise me and tell me much on DOs and DON'T s. Cause I passed through hell before getting this job.

Akintayo: alright..........

(Mr Akintayo lecturing me, I will wait till I see that He's saying all he knows, once I'm sure, I will be directing the discussion.)

Rotimi: Brother, is it not that Supervisors do visit?

Akintayo: They do visit o.

Rotimi: without giving notification?

Akintayo: they won't o.

Rotimi: they? So, not even one supervisor?

Akintayo: sometimes one and maybe more than that.

(I just found out I can act alone)

Rotimi: God will help sha.

Akintayo: Amen! Don't worry!

Rotimi: brother, how are you going to know they are supervisor? There should be a way to identify them.

Akintayo: ID CARD...

(Just found out I need to forge ID CARD, or do another social engineering to bypass it)

Rotimi: once I see a man in suit with an ID CARD coming in, SUPERVISION start niyen ọ

Akintayo: No o, They do wear branded shirts. Customised Polo shirts.

(I need that also..... The conversation continue, until I know all I want to know)

Naturally, we do want to be kind and grant help. But we shouldn't forget there is need to be careful. I will urge everyone to know who he or she is passing information to, whether the informations seem relevant or irrelevant, especially when the person is driving the discussion.

Pretexting

3. Pretexting

This is usually used to get information by giving the victim made-up reason, thus hide the true reason. The Social Engineer does appear as someone in need of help in this kind of method.

Example:

Let assume , I want to add a number as admin here and I don't have the privilege. Now, I will target two admins that are not that close, to avoid voice recognition or use a means to adjust my voice. I'm calling Gold.....

Gold: Hello

Rotimi: Yeah, Gold. I mistakenly removed a number from admin, and CS noticed this, He called me and chastened me, that did I want to cause problem, what If He his online, seeing me removing him.

Gold: ..... So, what.........(Trying to talk)

Rotimi: Just listen, I'm using someone phone, my phone went dead after dropping CS call. And had already asked him to help me add the number back, but He said He is busy, and not online now, that I should make sure I add the number back before he comes online. Just think of you as the best person to help, please help me add the number back , before he comes online, I don't want any trouble. I will send the number now....

(I ll end the call, not giving Mr Gold any chance to speak, and I may give him, it depends on my strategy)

If Mr Gold buy my story, then I will gain admin privileges. An Hacker is going to add another number as admin anyway, incase, Mr Gold found the truth from CS. If he removed the number, I ll still be admin with another number, that's called Persistence (Category: Maintaining Access)

4. Cold Calling.

Cold calling is actually when the attacker call claiming what He is not.

It's two Edged sword.

1. Targeting less vulnerable person through vulnerable person.

Example: I want to target Sir Rufai using my brother Niyi .I'm going to call

Rotimi: Hello

Skyrtel: Hello

(Through research I know they have technician)

Rotimi: I'm the Technician, I will like to speak with the Boss.

(My primary aim is to avoid questioning from Sir Rufai. According to my research He is difficult to deal with, I will be using Niyi to ease my work because he has limited knowledge on the technician. When Niyi is passing the call to Sir Rufai, He also passed the caller's info without verification. There is high probability that Sir Rufai will accept the info and keep the questioning. And sometimes it just reduce the questioning.)

Everyone should make sure He/She verifies who exactly the caller is. Whether it's your Boss, Father, Mother, Sister, Brother and so on, that pass you his/her information, verify again.

2. This is calling your target directly, claiming to be offering technical support.

E.g. I'm going to call Debsol, who has an account with Dazuki bank.

Rotimi: Good evening Sir.

Debsol: Good evening!

Rotimi: My name is Rotimi Mark, calling from Dazuki bank.

Debsol: OK !

Rotimi: due to the regulatory compliance, KNOW YOUR CUSTOMER SERVICE (KYC) we need to update your Account information.

Debsol: OK.

(I will ask whatever I want to ask)

Do make sure you are passing informations to a verified Source.

Our next sub- topic is Social Engineers Techniques.

Social Engineering Techniques.

This is where you ll find difference between a fraudster and Hacker. It's easier to outsmart a fraudster than an Hacker. With just the knowledge of Social Engineers psychology, you are good to evade a fraudster.

1. Dumpster diving

This is a situation where a Social Engineer goto the organisation's dumpster and collect all the papers for analysis. Sometimes, people write their passwords, usernames on papers and disposed it.

2. Impersonating: pretending to be someone, maybe to gain access to a restricted area in an organisation.

3. Shoulder surfing:

Staying behind the victim, while he or she type username or password. Or looking into the Browser's URL box to see the username and password, assuming the website is configured to use GET method to send the data to the server.

4. Phishing: this is making copy of a legitimate website to collect data from the website users.

I Spear-Phishing : is targeting an individual or organisation by sending emails that look legitimate which contains links to phished page.

II Whaling: this is targeting a specific organisation, by sending complaint, review, feedback emails which contains malware or malicious links.

5. Baiting: this is dropping USB flash drive or disc with attractive and intriguing label in target organisation, which contains malware and the victim system will be infected via autorun or autoplay. Just imagine dropping a USB with this label on it " Dazuki bank private customer accounts" unawared bank worker is going to check what's inside the drive, thus inject malicious code to system, which will spread into the whole network.

To avoid phishing, try not to be clicking links sent to you , type the website URL yourself. Or be checking the URL thoroughly before you input your data.

I will try to cover ways to know if your system is attacked. that will be on Securing Smartphones and Computers

6. Interactive Voice Response: creating a legitimate sounding copy of an organisation IVR system. Prompt victim with phishing emails to verify the information using the copy of IVR, in other to appear legitimate to the victim.

7. Quid pro quo:

Making cold call as technical support in hopes of reaching someone with a problem, then direct victim to install malware or disclose private information.

8. Tailgating:

This is trying to get to a restricted access without required credentials, Indentity token. The attacker dress legitimate and thus is allowed to walk behind someone with legitimate access to enter legitimate area, maybe by catching the door before it closes. Or coming behind a legitimate person dressing like a technician, carrying heavy bag, this make the person that have legitimate access to open and hold the door for him.

Now on Securing Smartphones.

I'm going to be using Android phones in this lecture.

Root Access!

It's a blessing for an Hacker to find out the victim's Android phone is rooted. It's called Jailbreaking in IPHONES.

What does Root means?

Android operating system is based on Linux kernel. Linux is an Operating System like Windows. In Windows, you are familiar with admin. When I say admin privileges, you know what it means. In Linux, it's root.... Root privileges.

By default, the manufacturer lock the root access, that's why you can't removed system apps or preinstalled apps, cause it's installed as root i.e. admin. You are regular user, you can't removed them.

When you get your phone rooted, then you can remove any app. Infact, you can remove all applications on your phone, including system apps.

This is the problem with root access.

The manufacturer has already gave some system apps root access, any app with root access can collect data from any app on your phone.

Assuming an attacker find his way to install his malicious app on your rooted phone, then the app is going to be king and collect data from any app and send it to the attacker either through email or any configured way.

If your phone is rooted, try to download lucky patcher, it's not harmful file but for practical. If you are a game lover, download a game that requires you to buy coin. With lucky patcher that has root access it will manipulate the game data. Thus you will be able to buy coin for free. And it's also use to remove adverts from apps.

If you have a rooted Android, make sure you don't automatically give apps root access. Make sure you are prompted when any app require it, and always check the Apps that you give root Access.

There is a powerful tool called Keylogger, when it's installed with root access , then it can send all your other apps data to the attacker, e.g. inbox, sent message, WhatsApp message, Facebook message, infact the attacker will know all your passwords.

What if Keylogger is installed without root Access?

Actually, it's going to collect some data. Why?

By default, the manufacturer allow any app to request for some system apps data, like your message app, Gps, Call app and so on, thus the attacker's keylogger can collect your messages and know your location, and it will be sent to the attacker.

Prevention!

1. Download apps from reliable sources e.g. Google Play store.

2. Check the Apps review before downloading.

3. When installing the Application, in the installation process, you are going to be presented with all the services/app will have access to. If you installed it, then it can interact with all the presented apps.

You can actually remove any service that you don't want the installed app to have access to.

4. Restricting apps to have access to data, thus the keylogger can only gather your information, it will not be able to send it to attacker.

NoRoot Data Firewall is a good app to do that, and it will manage your data usage also, as it will only give data to the app you allow. Even I personally do give my phone's browser 1 hour to use data assuming I want to quickly use them except Opera that I gave full Access.

Note: a clever hacker may installed an malicious app with no Icon to show on the screen, and it will autorun. If your phone is rooted, then you can manage your autorun list. You can remove and hide.

I'm not asking anyone to root his or her phone as it void warranty. But for those of us that can't do without rooted phone, please take all precautions. And do check your app list, remove apps that is not useful for you or those that you don't know how they get into your phone, assuming they ain't system app.

Beware of Keylogger, whether you root your phone or not, it's going to have access to your messaging app, thus send your Bank alerts to the attacker.

The rest will be covered on SECURING COMPUTERS....

Computer Security.

Cyber security, also known as Computer security or IT security, and we can conclude that it is the protection of computer systems from the theft and damage to their hardware, software or information in a network, as well as from disruption or misdirection of their functions.

Today, We will be exploring different ways of attacking and protecting our Computers.

WHAT ARE WILL PROTECTING?

1. Hardware

2. Software

3. Information.

We will be applying CIA on this three areas, you should be reminded I gave full meaning of CIA yesterday. If you are employing Security expert , and you ask him or her the meaning of CIA, but couldn't give you the meaning. Such doesn't worth the job, look for somebody else. What every Hacker/ Cyber Security expert will have in mind is CIA. It's our Map or something that tell us what to do.

Confidentiality: your data is only accessible by authorised person.

Integrity: your data is intact, not modified , destroyed or manipulated by unauthorised person.

Availability: your data is available when needed by authorised person.

Do you know most of Computers in Nigeria are vulnerable?

Why?

I went to a Computer Engineer to get some disc, I was so fortunate to see this Engineer installing Window XP on a customer system. That's really funny! Window XP?

Microsoft doesn't support Window XP anymore, so, Hackers can discover thousands of vulnerabilities in it, without anyone patching it. Currently, Window XP is critically vulnerable to attacks. You don't install what's no longer supported by the vendor, because when a vulnerability is discovered in it, hackers will find a way to exploit the vulnerability and the vendor won't provide any patch or update to evade the vulnerability.

Window XP has bunches of vulnerabilities, though hackers don't even have time to find further vulnerability, at least, the known vulnerabilities are still useful and not patched by Microsoft.

Secondly, many Computer Engineers doesn't know much on hardware compatibility. My friend wanted to buy a laptop and gave me a call to get him one, but I couldn't meet the time given. He went somewhere else, but He called me to gave him direction on what to buy. I wanted him to buy 64bit system. I had to join him at the place when the Engineer couldn't understand my language. Our conversation was like this,

Rotimi: I was telling you we want 64bit system.

Engineer: we have 32bit but I can upgrade it.

Rotimi: do you know what I'm saying?

(I was imagining if he can actually replace motherboard and CPU)

Engineer: I will install it, but 32bit is OK.

(Another friend of ours, who is also an Engineer was trying to explain what he meant)

Ridwan: He will install 64bit software to it now. Lekan, 32bit is OK.

I got muted , seriously funny.

We have 32bit and 64bit processor, upgrading from 32bit means you are replacing the processor. And many other hardwares should be checked for compatibility before upgrading, especially motherboard compability. And necessary 64bit drivers should be installed.