UKaid
from the British people

DigiGirls

Module Introduction

An initiative of
cybersafe.
FOUNDATION

UKaid
from the British people

DigiGirls

Content

- Some fun facts
- What is Cybersecurity awareness
- Course Outline
- Learning outcome

An initiative of
cybersafe.
FOUNDATION

UKaid
from the British people

DigiGirls

Some Facts...

- It is estimated that cybercrime will cost the global economy more than 20 trillion U.S dollars by 2026, a 1.5 times increase compared to figures in 2022 (Source: Statista)
- The latest study by cybersecurity company Surfshark has revealed that the incidences of data breaches in Nigeria increased by 64% in Q1, 2023.
- Nigeria has been ranked as the 32nd most breached country from January to March 2023 (Q1'2023).
- Globally, a total of 41.6M accounts were breached in Q1'2023, with Russia ranking first and amounting to a sixth of all breaches from January through March.

An initiative of
cybersafe.
FOUNDATION

UKaid
from the British people

DigiGirls

What is Cybersecurity Awareness?

Cybersecurity awareness refers to how much technology users know about the cyber security threats, risks and mitigating best practices to guide behavior.

This is particularly important because end users are considered the first line of defense against certain cybersecurity attacks .

An initiative of
cybersafe.
FOUNDATION

Course Outline

- Introduction to Cybersecurity and Responsible Digital Citizenship
- Avoiding Social Engineering Attacks and Protecting from Cyber Fraud
- Protecting against viruses and other malware
- Keeping your smartphone, tablets and computers safe
- Keeping your online accounts secure
- Protection Against IoT and AI Attacks

An initiative of cybersafe. FOUNDATION

UKaid
from the British people

DigiGirls

Learning Outcomes

- Understand basic cybersecurity concepts
- Learn how to protect yourself and your organizations from the most prevalent cyber attacks
- Understand and apply various data and device protection methods
- Gain safe web browsing and social media practice and other cyber hygiene habits
- Understand how to use IoT devices and AI tools safely.

UKaid
from the British people

DigiGirls

THANK YOU

An initiative of
cybersafe.
FOUNDATION

UKaid
from the British people

DigiGirls

Introduction to Cybersecurity and Responsible Digital Citizenship

An initiative of
cybersafe.
FOUNDATION

UKaid
from the British people

DigiGirls

Content

- Cyber Security Myths vs Truths
- Basic Cybersecurity concepts
- Prevalent Cyber Threats and Attacks
- Impacts of Cyber Attacks on Businesses
- Responsible Use of Digital

An initiative of
cybersafe.
FOUNDATION

UKaid
from the British people

DigiGirls

Cyber Security Myths vs Truths

An initiative of
cybersafe.
FOUNDATION

UKaid
from the British people

DigiGirls

Everyone who uses technology is at risk of being a victim of Cybercrime

I don’t have plenty money, I am not famous, It’s unlikely that I will ever experience a cyber attack

An initiative of
cybersafe.
FOUNDATION

UKaid
from the British people

DigiGirls

This is as good as fetching water with a basket or going to sleep with your back door left wide open

Having a free or cracked anti-virus software is enough to protect me

An initiative of
cybersafe.
FOUNDATION

UKaid
from the British people

DigiGirls

Cybersecurity is everyone's responsibility

Cyber security is the responsibility of only tech people.

An initiative of
cybersafe.
FOUNDATION

UKaid
from the British people

DigiGirls

This is risky behaviour and could lead to your account being hacked

It is okay to use my birthday, pet name or even my name as my birthday

An initiative of
cybersafe.
FOUNDATION

UKaid
from the British people

DigiGirls

It is okay to use the same password across all my online accounts

You'll make it really easy for cybercriminals to compromise multiple accounts that belong to you

An initiative of
cybersafe.
FOUNDATION

UKaid
from the British people

DigiGirls

Password is often not enough; you need to turn on multi-factor authentication everywhere possible

I use a strong password, that should be enough to protect me

An initiative of
cybersafe.
FOUNDATION

UKaid
from the British people

DigiGirls

Cybercriminals are getting better at tricking people who are not aware of their tactics. Being Cyber aware, keeps you a step ahead

I am too street smart for any online scammer to defraud me, I don't need to learn about cybersecurity

An initiative of cybersafe. FOUNDATION

www.haveibeenpwned.com

UKaid
from the British people

DigiGirls

https://www.f-secure.com/en/identity-theft-checker

An initiative of
cybersafe.
FOUNDATION

THANK YOU

UKaid
from the British people

DigiGirls

Basic Cybersecurity Concepts

An initiative of
cybersafe.
FOUNDATION

Cybersecurity as a Business Enabler

Cybersecurity refers to the application of technologies, processes and controls to protect systems, networks, programs, devices and data from cyber attacks.

UKaid
from the British people

DigiGirls

An initiative of cybersafe. FOUNDATION

Cyber Attack

A cyber attack is any attempt to gain unauthorized access to a computer, computing system or computer network with the intent to cause damage.

An initiative of cybersafe. FOUNDATION

UKaid
from the British people

DigiGirls

Data Breach

Data breaches are security events where information is accessed, stolen, and used by a cybercriminal without authorization.

An initiative of cybersafe. FOUNDATION

Cyber Threat

A cyber or cybersecurity threat is a harmful act that seeks to damage data, steal data, or disrupt digital life in general.

Cyber Crime

Cybercrime is defined as a crime in which a computer is used as a tool to commit an offence. Criminals who perform these illegal activities are often referred to as **cyber criminals.**

UKaid
from the British people

DigiGirls

THANK YOU

An initiative of
cybersafe.
FOUNDATION

UKaid
from the British people

DigiGirls

Prevalent Cyber Threats and Attacks

An initiative of
cybersafe.
FOUNDATION

UKaid
from the British people

DigiGirls

Top 5 Cybersecurity Threats in Africa

Online Scams

Ransomware

Botnets

Business Email Compromise

Digital Extortion

An initiative of
cybersafe.
FOUNDATION

UKaid
from the British people

DigiGirls

About Online Scams

A cyber or cybersecurity threat is a harmful act that seeks to damage data, steal data, or disrupt digital life in general.

An initiative of
cybersafe.
FOUNDATION

Cyber Threats : Online Scams

Phishing/Smishing/Vishing, debit/credit card theft, identity theft, advance payment fraud, fraud, investment scams, cryptocurrency scams, etc.

Attackers use of deceptive means that include stirring emotions and manipulating people into taking harmful decisions and divulging sensitive information. What do they want? Your identity, money, sensitive information and online accounts.

Cyber Threats : Digital Extortion

Blackmailing + Sextortion + False Information

False claims or proof of stolen personal data or files, for which the victim is then asked to pay in exchange for recovering the data or not leaking it online.

Cyber Threats : Business Email Compromise

Cybercriminals typically compromise or spoof a legitimate email account to send fraudulent emails requesting transfer of funds or sensitive data while posing as the legitimate owner of the email account.

Cybercriminals usually target high-level executives working in finance or involved with wire transfer payments. Bogus Invoices, CEO Fraud, Account Compromise.

UKaid
from the British people

DigiGirls

Cyber Threats : Botnets

A Botnet is a network of hijacked computers and devices infected with harmful code and remotely controlled by a hacker.

Botnets can also be an entry point for ransomware attacks. Any machine that can connect to the Internet can be compromised and turned into a device in a botnet, such as computers, mobile devices, internet infrastructure hardware such as network routers, and increasingly, Internet-of-Things (IoT) devices such as smart home devices.

An initiative of
cybersafe.
FOUNDATION

Cyber Threats : Ransomware

Ransomware is a form of malware which encrypts victim data or locks down systems, disrupting the operations of victim organizations by rendering their data and systems inaccessible.

THANK YOU

UKaid
from the British people

DigiGirls

Impacts of Cyber Attacks on Businesses

An initiative of
cybersafe.
FOUNDATION

Impacts of Cyber Attacks on Business

A successful cyber attack can impact the entire organization in many ways and on many levels, from minor operational disruption to a total business meltdown. Some of the ways cybercrime can hamper businesses include:

- Financial losses; cost of response and recovery, cost of investigation, cost of loss productivity, lost revenue, legal and PR costs
- Loss of customer’s confidential information and crucial business information
- Reputation damage
- Loss of productivity
- Legal liability
- Business Continuity problems

UKaid
from the British people

DigiGirls

Impact above the surface

Well-known cyber incident costs

- Customer breach notifications
- Post breach customer protection
- Regulatory compliance (fines)
- Public relations/crisis communications
- Attorney fees and litigation
- Cybersecurity improvements
- Technical investigations

Impact below the surface

Hidden or less visible costs

- Insurance premium increases
- Increased cost to raise debt
- Operational disruption or destruction
- Lost value of customer relationships
- Value of lost contract revenue
- Devaluation of trade name
- Loss of intellectual property (IP)

An initiative of
cybersafe.
FOUNDATION

Actionable Tips To Protect Yourself

1. Know how to identify scam emails from Legitimate one
2. Backup your files securely online and offline
3. Strengthen your home network and avoid using Public WiFi
4. Use strong passwords
5. Keep software updated especial Windows updates, web browser, etc
6. Use 2-Factor Authentication on your social media and email accounts
7. Install and use a good anti-virus
8. Catch red flags such as unexplained urgency, last minute changes to wire-instructions or established communication channels or refusal to communicate via video calls.
9. Don’t download files, software or apps from shady websites.

THANK YOU

UKaid
from the British people

DigiGirls

An initiative of
cybersafe.
FOUNDATION

UKaid
from the British people

DigiGirls

Responsible Use of Digital

An initiative of
cybersafe.
FOUNDATION

UKaid
from the British people

DigiGirls

Cybersecurity is everyone’s responsibility

Do you know?

An initiative of
cybersafe.
FOUNDATION

Responsible Use of Digital

- Secure your secrets (Online security and passwords)
- Share with care and caution
- Be Kind Online
- Don’t fall for fake (Online scams, fake news, etc.)
- When in doubt, verify

An initiative of cybersafe. FOUNDATION

UKaid
from the British people

DigiGirls

Topic Activity

In your peer learning groups, discuss how a cyber-attack can cause harm to your favorite business in your community.

An initiative of
cybersafe.
FOUNDATION

UKaid
from the British people

DigiGirls

THANK YOU

An initiative of
cybersafe.
FOUNDATION

UKaid
from the British people

DigiGirls

Avoiding Social Engineering Attacks and Protecting from Cyber Fraud

An initiative of
cybersafe.
FOUNDATION

UKaid
from the British people

DigiGirls

Content

- Social Engineering
- Social Engineering Methods
- Cyber Fraud

An initiative of
cybersafe.
FOUNDATION

SOCIAL ENGINEERING

UKaid
from the British people

DigiGirls

An initiative of
cybersafe.
FOUNDATION

Social Engineering

- Psychology of Social Engineering
- Social Engineering Case Study

An initiative of cybersafe. FOUNDATION

UKaid
from the British people

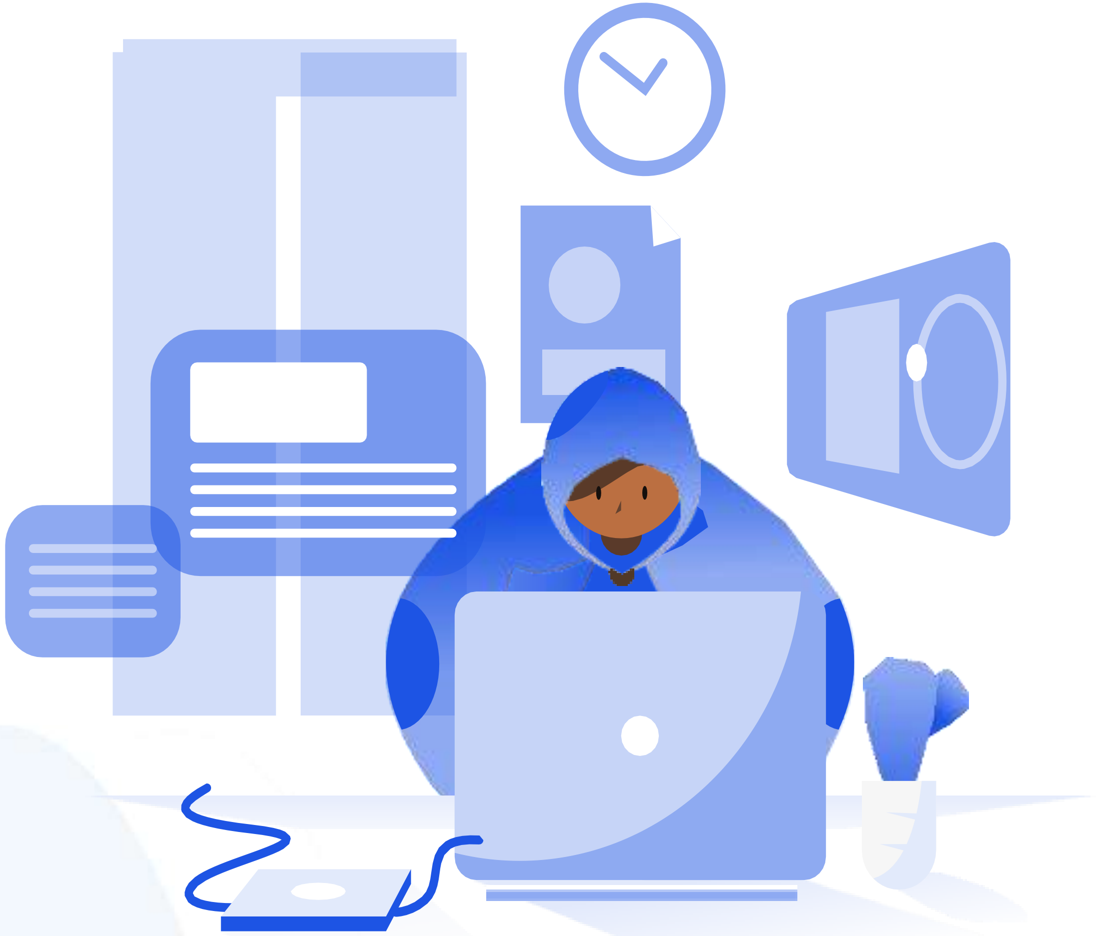
DigiGirls

Psychology of Social Engineering

An initiative of
cybersafe.
FOUNDATION

What is Social Engineering?

The art of psychologically manipulating people into making security mistakes, divulging confidential/sensitive information or taking harmful actions.



An initiative of cybersafe. FOUNDATION

Let’s take a look at the facts

Nigeria’s Consumer Awareness and Financial Enlightenment Initiative had projected a $6tn loss by 2030 to cybercrime within and outside Nigeria. These crimes are committed mostly through phishing and identity theft.

Social Engineering is the #1 Cyber threat faced in Nigeria

Emotions

(Desire, Fear, Greed, urgency, Panic, Excitement, Trust , Curosity)

An initiative of cybersafe. FOUNDATION

Why hack technology if it’s easier to hack a human?

What Do They Want

- Your identity
- Your money
- Sensitive information
- Online accounts

UKaid
from the British people

DigiGirls

THANK YOU

An initiative of
cybersafe.
FOUNDATION

UKaid
from the British people

DigiGirls

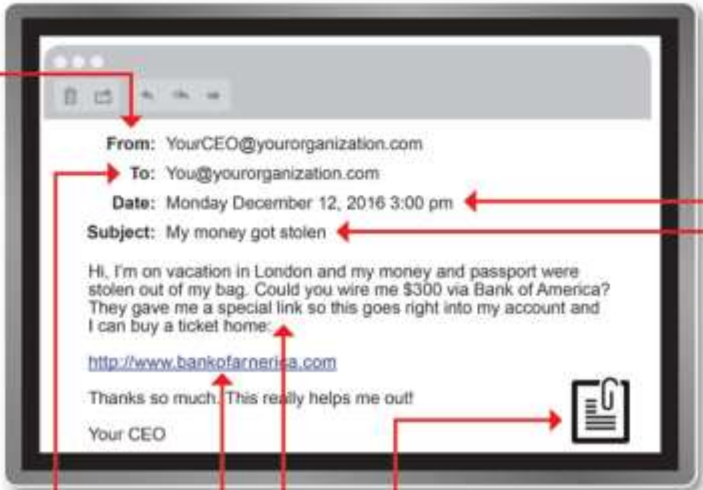
Social Engineering Case Study

An initiative of
cybersafe.
FOUNDATION

UKaid
from the British people

Social Engineering Red Flags

DigiGirls



From: YourCEO@yourorganization.com
To: You@yourorganization.com
Date: Monday December 12, 2016 3:00 pm
Subject: My money got stolen

Hi, I'm on vacation in London and my money and passport were stolen out of my bag. Could you wire me $300 via Bank of America? They gave me a special link so this goes right into my account and I can buy a ticket home:

http://www.bankofarnerica.com

Thanks so much. This really helps me out!

Your CEO

FROM

- I don't recognize the sender's email address as someone **I ordinarily communicate with**.
- This email is from **someone outside my organization and it's not related to my job responsibilities**.
- This email was sent from **someone inside the organization** or from a customer, vendor, or partner and is **very unusual or out of character**.
- Is the sender's email address from a **suspicious domain** (like micorsoft-support.com)?
- **I don't know the sender personally** and they **were not vouched for** by someone I trust.
- **I don't have a business relationship** nor any past communications with the sender.
- This is an **unexpected or unusual email** with an **embedded hyperlink or an attachment** from someone I haven't communicated with recently.

TO

- I was cc'd on an email sent to one or more people, but **I don't personally know** the other people it was sent to.
- I received an email that was also sent to an **unusual mix of people**. For instance, it might be sent to a random group of people at my organization whose last names start with the same letter, or a whole list of unrelated addresses.

HYPERLINKS

- I hover my mouse over a hyperlink that's displayed in the email message, but the **link-to address is for a different website**. (This is a **big** red flag.)
- I received an email that only has **long hyperlinks with no further information**, and the rest of the email is completely blank.
- I received an email with a **hyperlink that is a misspelling** of a known web site. For instance, www.bankofarnerica.com — the "m" is really two characters — "r" and "n."

DATE

- Did I receive an email that I normally would get during regular business hours, but it was **sent at an unusual time** like 3 a.m.?

SUBJECT

- Did I get an email with a subject line that is **irrelevant** or **does not match** the message content?
- Is the email message a reply to something **I never sent or requested**?

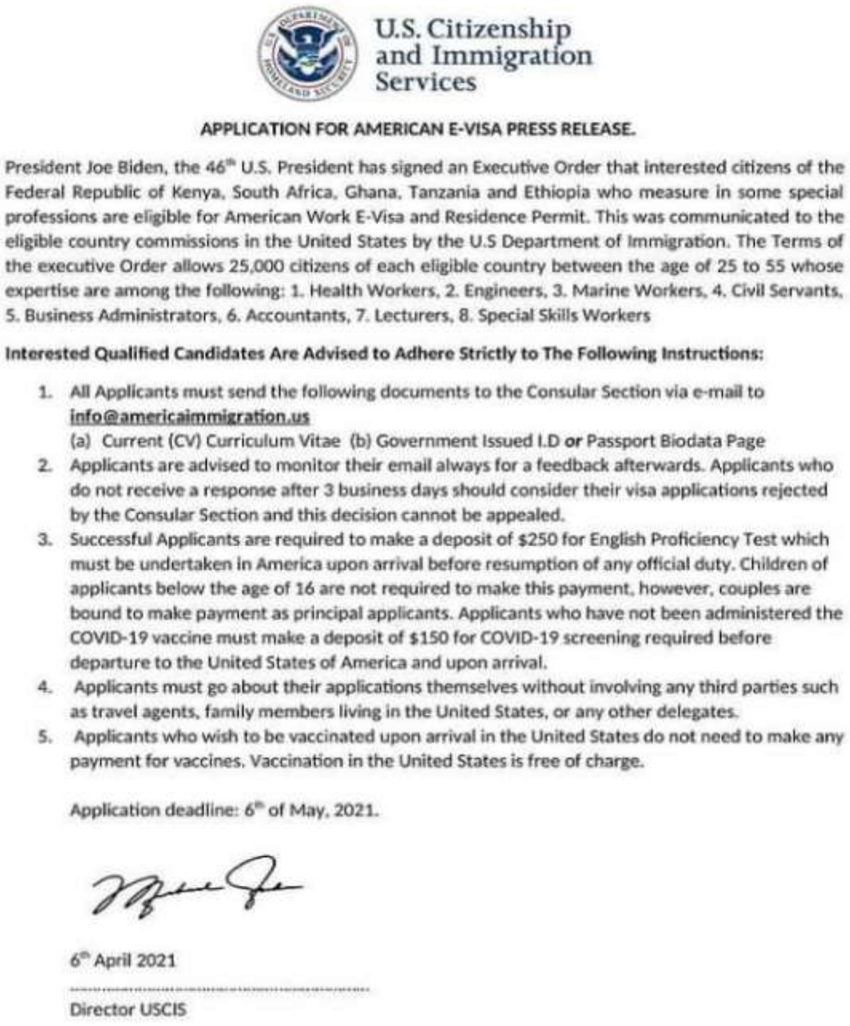
ATTACHMENTS

- The sender included an email attachment that **I was not expecting** or that **makes no sense** in relation to the email message. (This sender doesn't ordinarily send me this type of attachment.)
- I see an attachment with a possibly **dangerous file type**. The only file type that is **always safe to click on is a .txt** file.

CONTENT

- Is the sender asking me to click on a link or open an attachment to **avoid a negative consequence** or to **gain something of value**?
- Is the email **out of the ordinary**, or does it have **bad grammar** or **spelling errors**?
- Is the sender asking me to click a link or open up an attachment that **seems odd** or **illogical**?
- Do I have an **uncomfortable gut feeling** about the sender's request to open an attachment or click a link?
- Is the email asking me to look at a **compromising or embarrassing picture** of myself or someone I know?

An initiative of
cybersafe.
FOUNDATION



U.S. Citizenship and Immigration Services

APPLICATION FOR AMERICAN E-VISA PRESS RELEASE.

President Joe Biden, the 46th U.S. President has signed an Executive Order that interested citizens of the Federal Republic of Kenya, South Africa, Ghana, Tanzania and Ethiopia who measure in some special professions are eligible for American Work E-Visa and Residence Permit. This was communicated to the eligible country commissions in the United States by the U.S Department of Immigration. The Terms of the executive Order allows 25,000 citizens of each eligible country between the age of 25 to 55 whose expertise are among the following: 1. Health Workers, 2. Engineers, 3. Marine Workers, 4. Civil Servants, 5. Business Administrators, 6. Accountants, 7. Lecturers, 8. Special Skills Workers

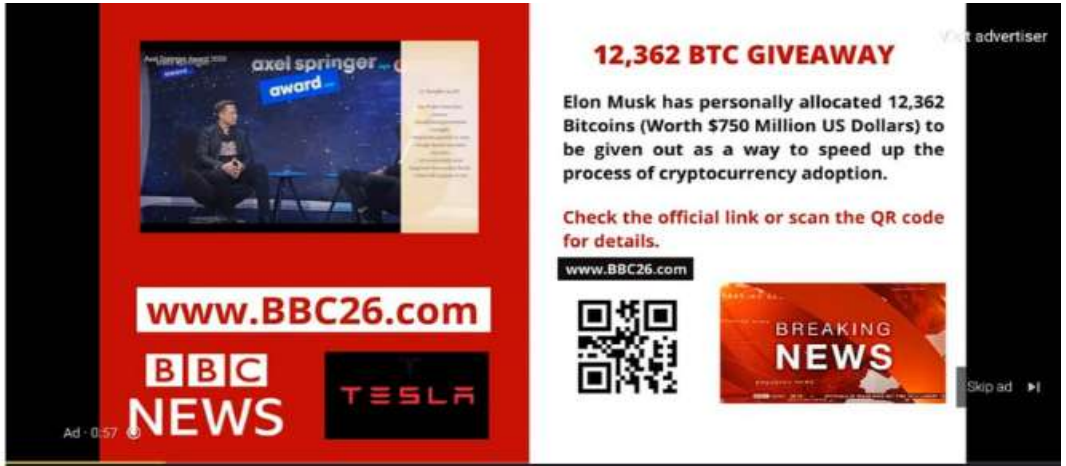
Interested Qualified Candidates Are Advised to Adhere Strictly to The Following Instructions:

1. All Applicants must send the following documents to the Consular Section via e-mail to **info@americaimmigration.us**
   (a) Current (CV) Curriculum Vitae (b) Government Issued I.D **or** Passport Biodata Page
2. Applicants are advised to monitor their email always for a feedback afterwards. Applicants who do not receive a response after 3 business days should consider their visa applications rejected by the Consular Section and this decision cannot be appealed.
3. Successful Applicants are required to make a deposit of $250 for English Proficiency Test which must be undertaken in America upon arrival before resumption of any official duty. Children of applicants below the age of 16 are not required to make this payment, however, couples are bound to make payment as principal applicants. Applicants who have not been administered the COVID-19 vaccine must make a deposit of $150 for COVID-19 screening required before departure to the United States of America and upon arrival.
4. Applicants must go about their applications themselves without involving any third parties such as travel agents, family members living in the United States, or any other delegates.
5. Applicants who wish to be vaccinated upon arrival in the United States do not need to make any payment for vaccines. Vaccination in the United States is free of charge.

Application deadline: 6th of May, 2021.

6th April 2021

Director USCIS

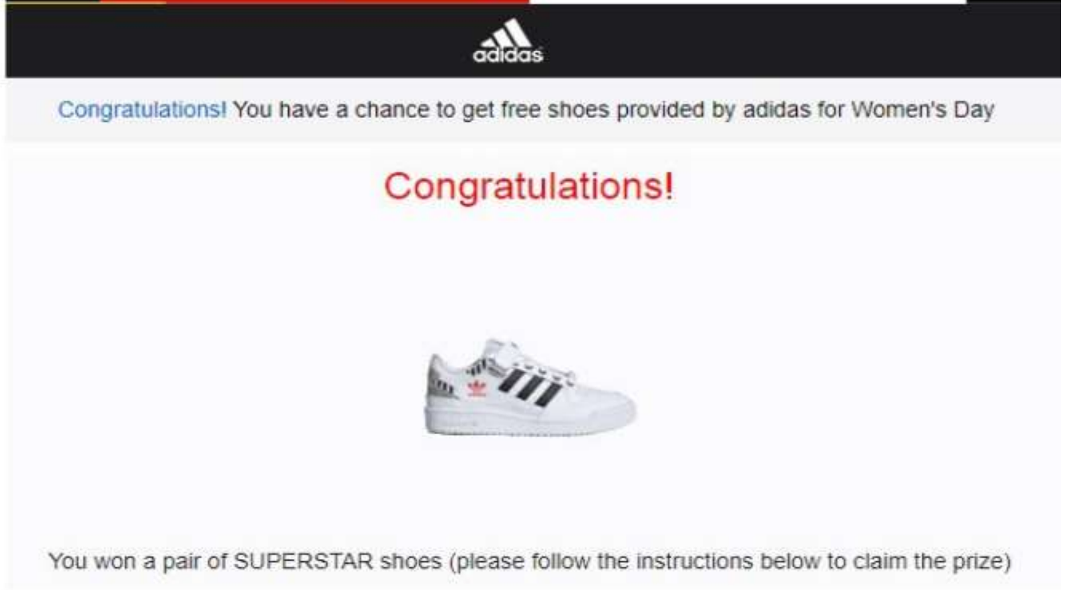


12,362 BTC GIVEAWAY

Elon Musk has personally allocated 12,362 Bitcoins (Worth $750 Million US Dollars) to be given out as a way to speed up the process of cryptocurrency adoption.

Check the official link or scan the QR code for details.

www.BBC26.com



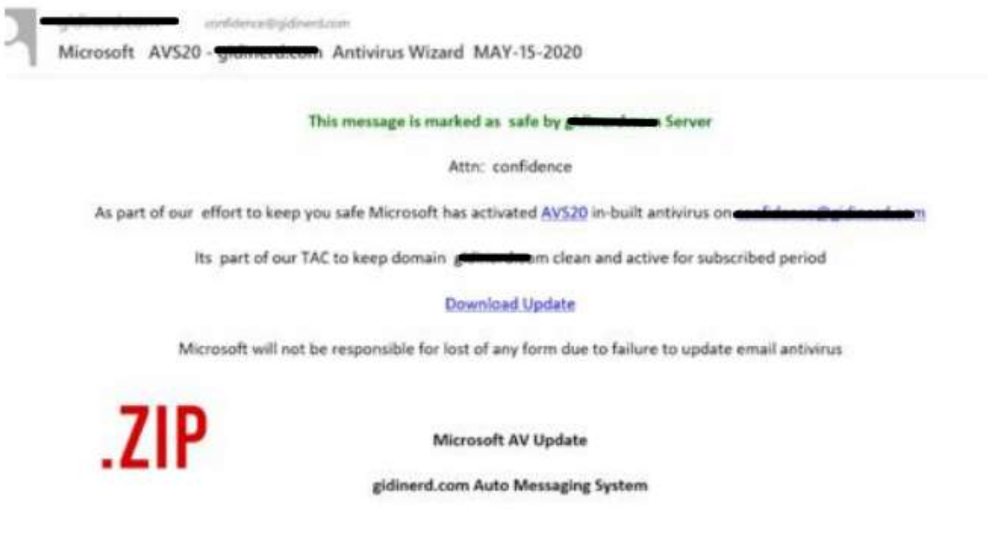
Congratulations! You have a chance to get free shoes provided by adidas for Women's Day

Congratulations!

You won a pair of SUPERSTAR shoes (please follow the instructions below to claim the prize)

UKaid
from the British people

DigiGirls



[redacted] confidence@gidinerd.com

Microsoft AVS20 - [redacted] Antivirus Wizard MAY-15-2020

This message is marked as safe by [redacted] Server

Attn: confidence

As part of our effort to keep you safe Microsoft has activated AVS20 in-built antivirus on [redacted]

Its part of our TAC to keep domain [redacted] clean and active for subscribed period

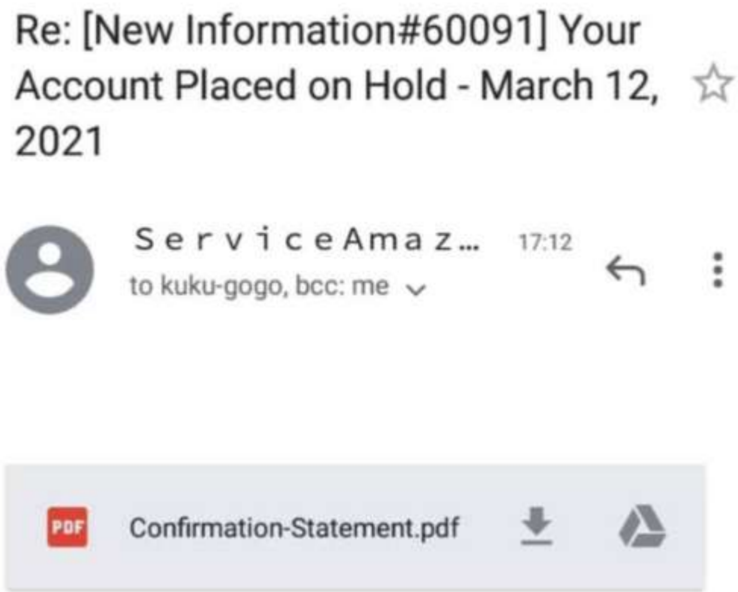
Download Update

Microsoft will not be responsible for lost of any form due to failure to update email antivirus

.ZIP

Microsoft AV Update

gidinerd.com Auto Messaging System

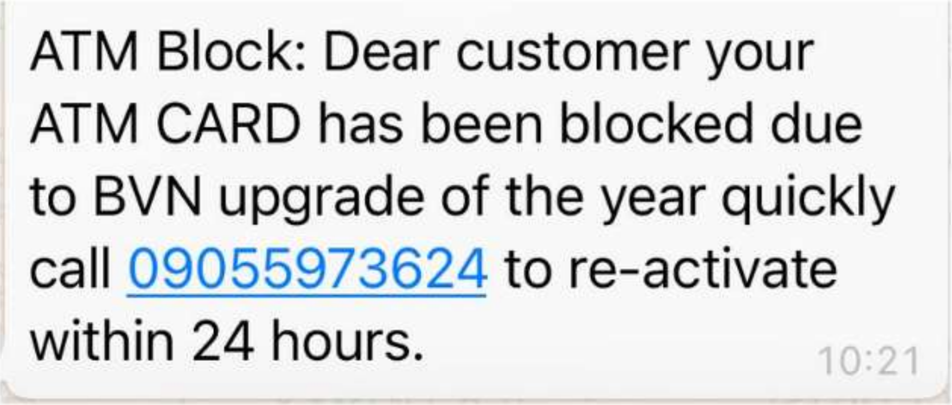


Re: [New Information#60091] Your Account Placed on Hold - March 12, 2021

ServiceAmaz... 17:12

to kuku-gogo, bcc: me

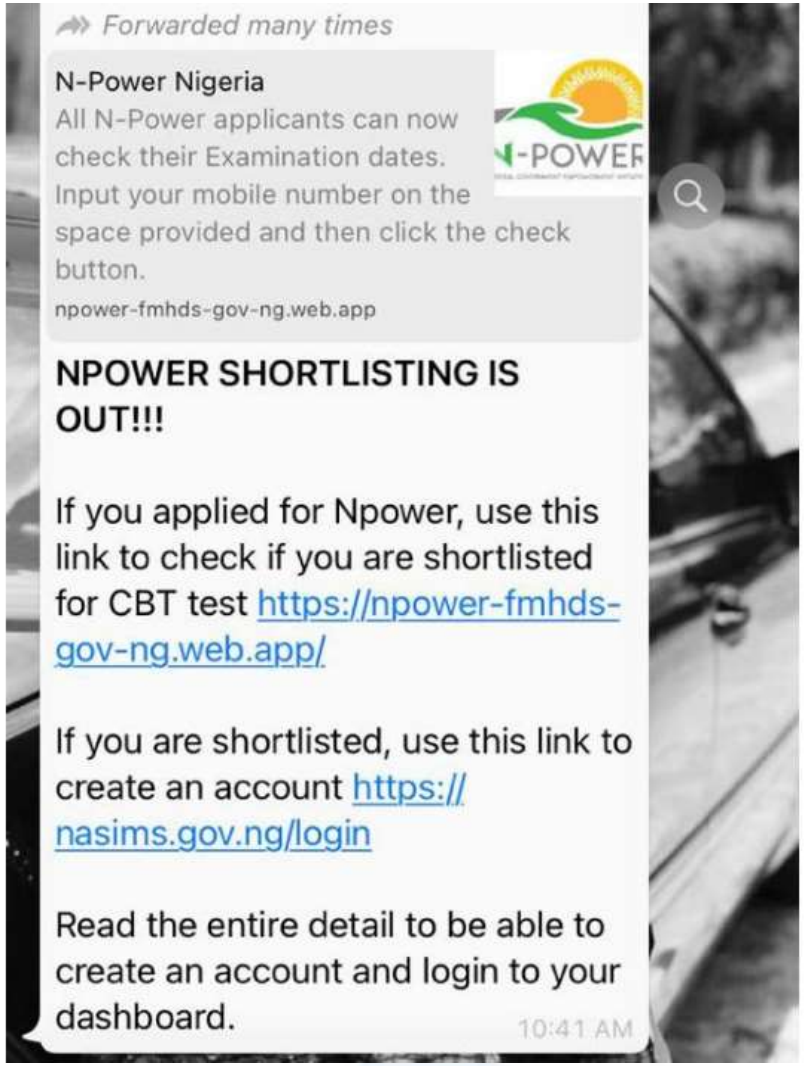
Confirmation-Statement.pdf



ATM Block: Dear customer your ATM CARD has been blocked due to BVN upgrade of the year quickly call 09055973624 to re-activate within 24 hours.

10:21

An initiative of
cybersafe.
FOUNDATION



Forwarded many times

N-Power Nigeria

All N-Power applicants can now check their Examination dates. Input your mobile number on the space provided and then click the check button.

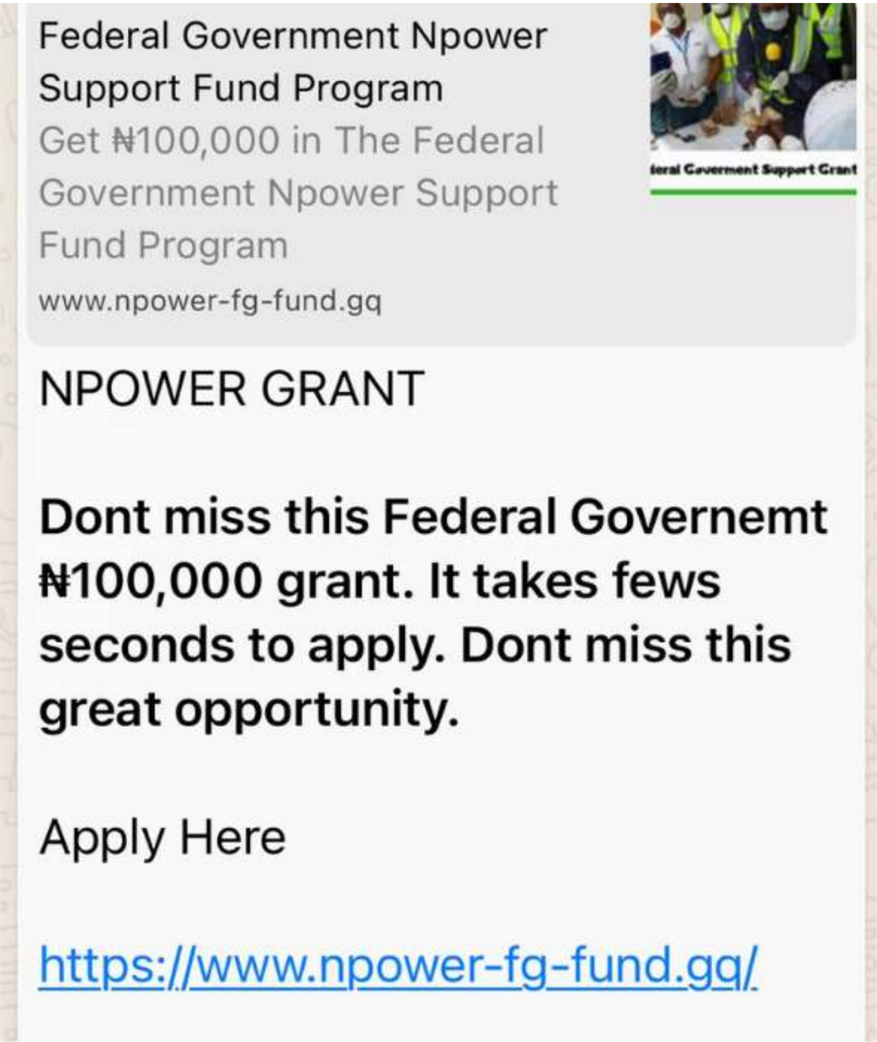
npower-fmhds-gov-ng.web.app

NPOWER SHORTLISTING IS OUT!!!

If you applied for Npower, use this link to check if you are shortlisted for CBT test https://npower-fmhds-gov-ng.web.app/

If you are shortlisted, use this link to create an account https://nasims.gov.ng/login

Read the entire detail to be able to create an account and login to your dashboard. 10:41 AM



Federal Government Npower Support Fund Program

Get ₦100,000 in The Federal Government Npower Support Fund Program

www.npower-fg-fund.gq

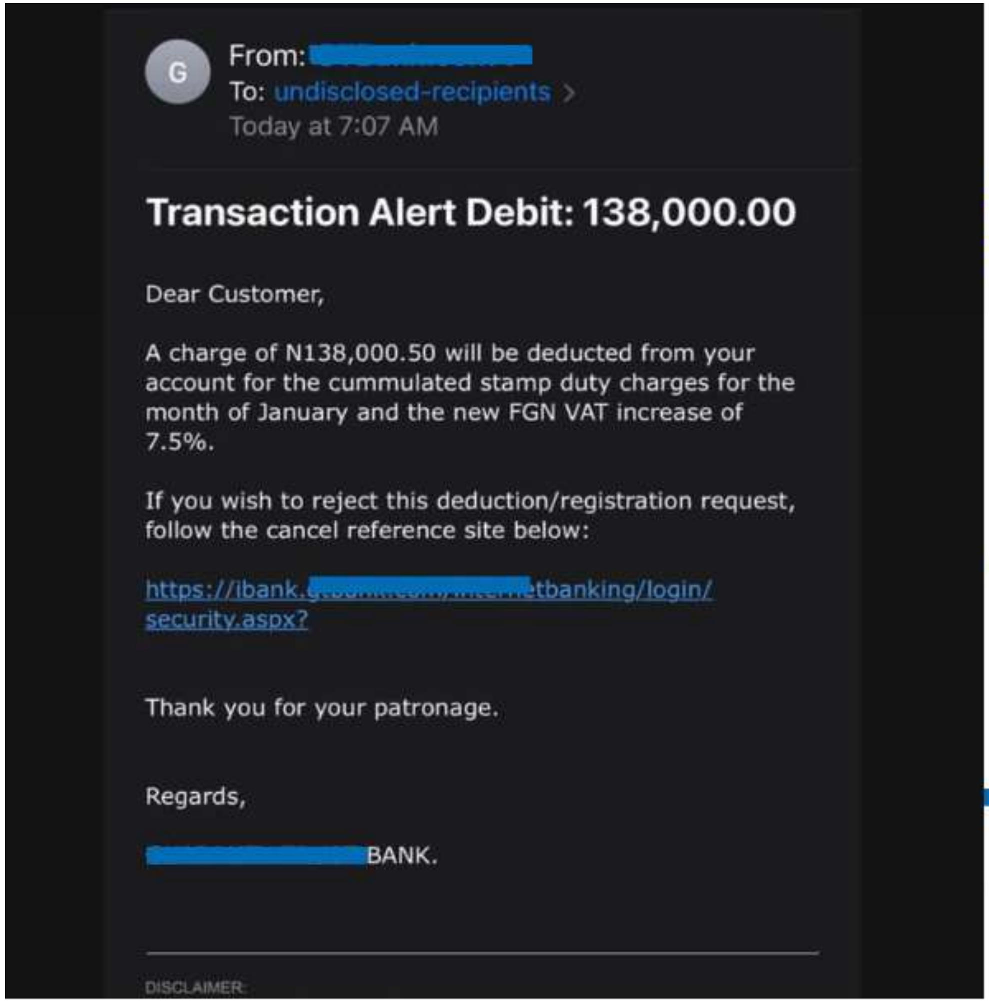
NPOWER GRANT

Dont miss this Federal Governemt ₦100,000 grant. It takes fews seconds to apply. Dont miss this great opportunity.

Apply Here

https://www.npower-fg-fund.gq/

An initiative of cybersafe. FOUNDATION



From: [redacted]
To: undisclosed-recipients
Today at 7:07 AM

Transaction Alert Debit: 138,000.00

Dear Customer,

A charge of N138,000.50 will be deducted from your account for the cummulated stamp duty charges for the month of January and the new FGN VAT increase of 7.5%.

If you wish to reject this deduction/registration request, follow the cancel reference site below:

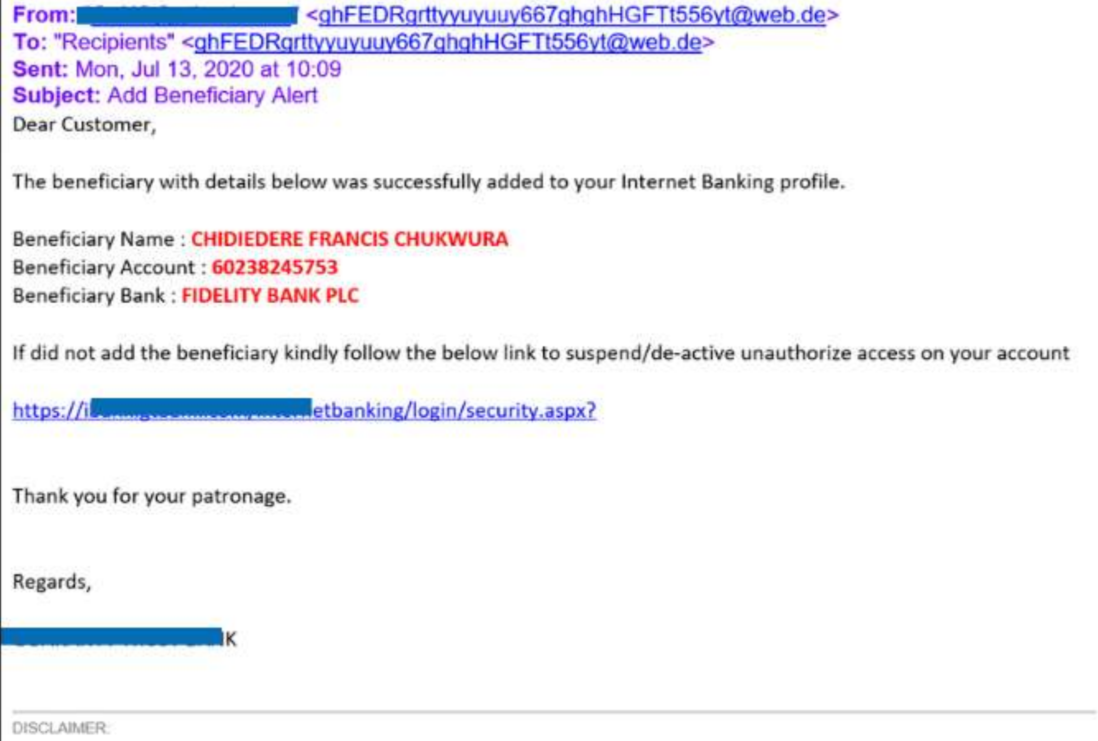
https://ibank.[redacted]etbanking/login/security.aspx?

Thank you for your patronage.

Regards,

[redacted]BANK.

DISCLAIMER:



From: [redacted] <ghFEDRgrttyyuyuuy667ghghHGFTt556yt@web.de>
To: "Recipients" <ghFEDRgrttyyuyuuy667ghghHGFTt556yt@web.de>
Sent: Mon, Jul 13, 2020 at 10:09
Subject: Add Beneficiary Alert

Dear Customer,

The beneficiary with details below was successfully added to your Internet Banking profile.

Beneficiary Name : **CHIDIEDERE FRANCIS CHUKWURA**
Beneficiary Account : **60238245753**
Beneficiary Bank : **FIDELITY BANK PLC**

If did not add the beneficiary kindly follow the below link to suspend/de-active unauthorize access on your account

https://i[redacted]etbanking/login/security.aspx?

Thank you for your patronage.

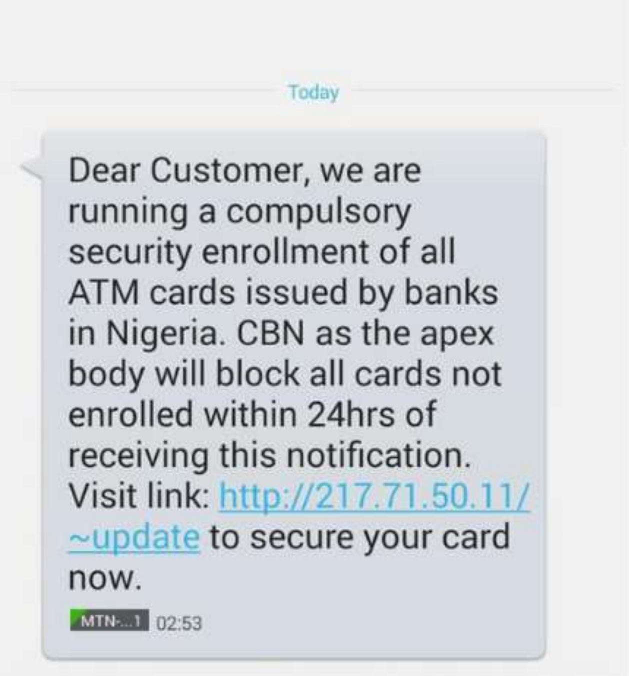
Regards,

[redacted]K

DISCLAIMER:

UKaid
from the British people

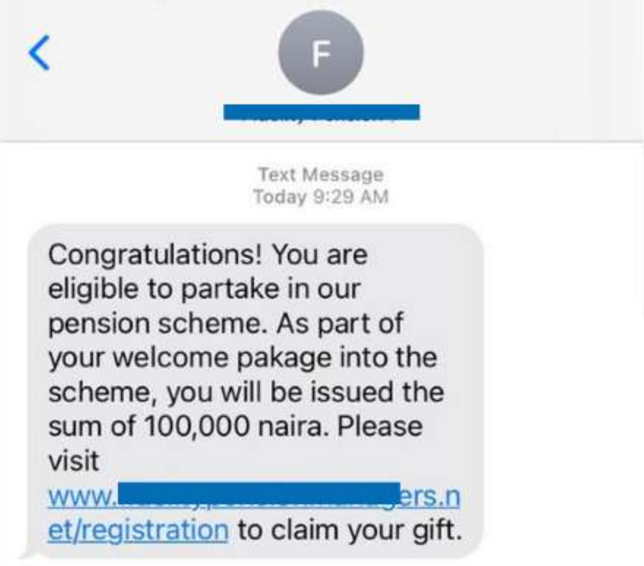
DigiGirls



Today

Dear Customer, we are running a compulsory security enrollment of all ATM cards issued by banks in Nigeria. CBN as the apex body will block all cards not enrolled within 24hrs of receiving this notification. Visit link: http://217.71.50.11/~update to secure your card now.

MTN-...1 02:53

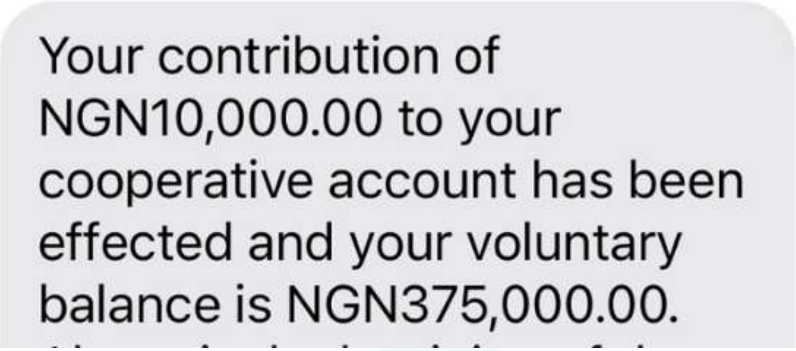


F

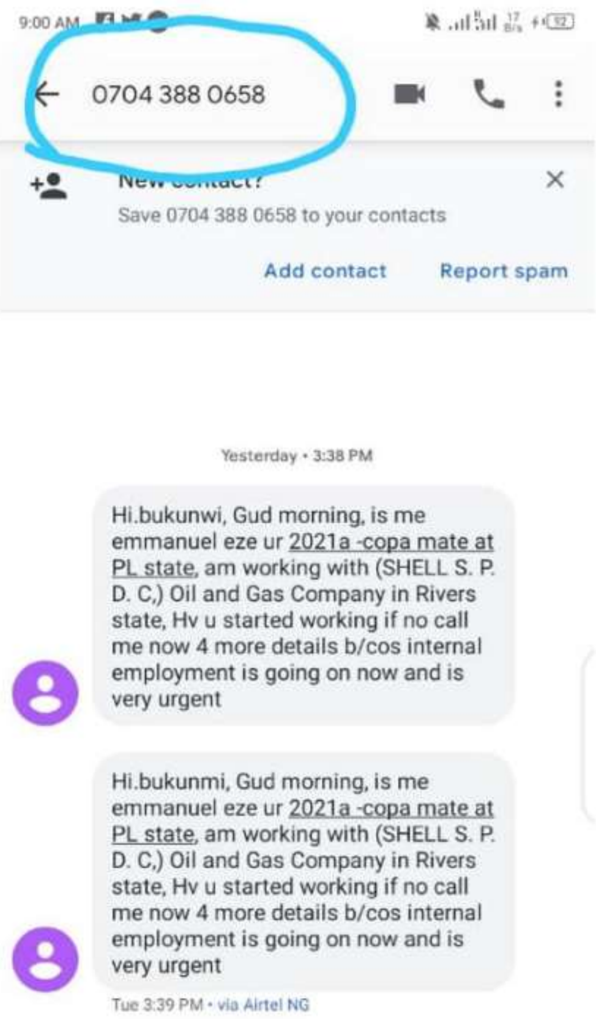
[redacted]

Text Message
Today 9:29 AM

Congratulations! You are eligible to partake in our pension scheme. As part of your welcome pakage into the scheme, you will be issued the sum of 100,000 naira. Please visit www.[redacted]ers.net/registration to claim your gift.



Your contribution of NGN10,000.00 to your cooperative account has been effected and your voluntary balance is NGN375,000.00.



9:00 AM

0704 388 0658

New contact?
Save 0704 388 0658 to your contacts

Add contact Report spam

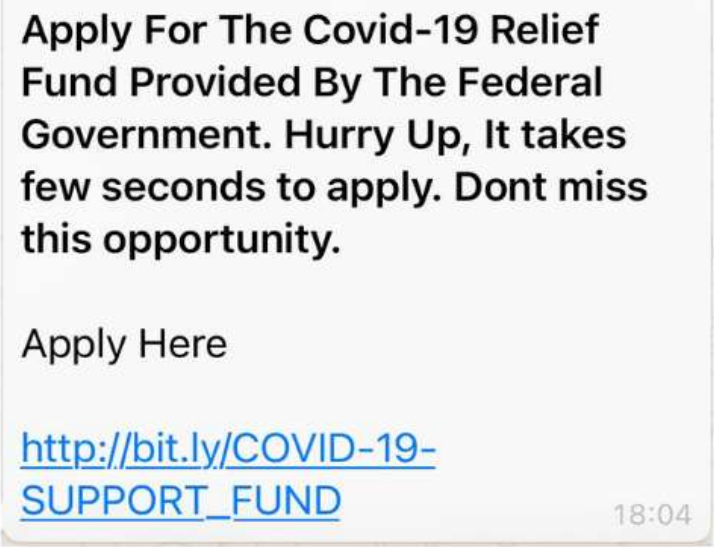
Yesterday • 3:38 PM

Hi.bukunwi, Gud morning, is me emmanuel eze ur 2021a -copa mate at PL state, am working with (SHELL S. P. D. C,) Oil and Gas Company in Rivers state, Hv u started working if no call me now 4 more details b/cos internal employment is going on now and is very urgent

Hi.bukunmi, Gud morning, is me emmanuel eze ur 2021a -copa mate at PL state, am working with (SHELL S. P. D. C,) Oil and Gas Company in Rivers state, Hv u started working if no call me now 4 more details b/cos internal employment is going on now and is very urgent

Tue 3:39 PM • via Airtel NG

An initiative of
cybersafe.
FOUNDATION

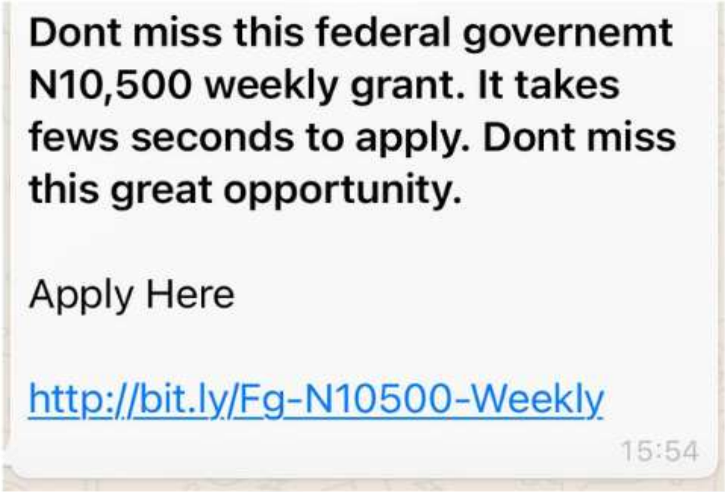


Apply For The Covid-19 Relief Fund Provided By The Federal Government. Hurry Up, It takes few seconds to apply. Dont miss this opportunity.

Apply Here

http://bit.ly/COVID-19-SUPPORT_FUND

18:04

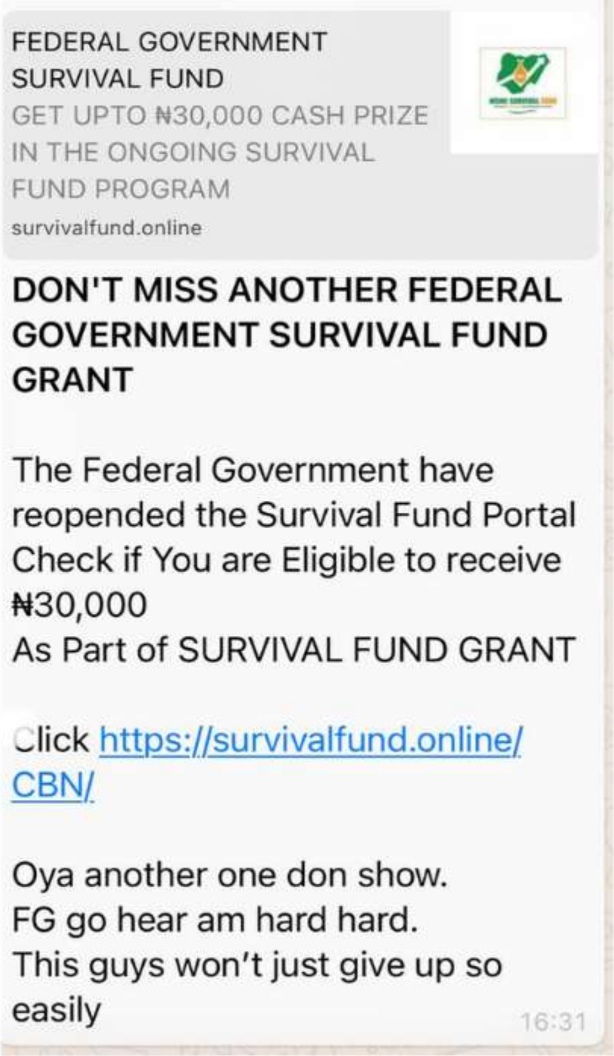


Dont miss this federal governemt N10,500 weekly grant. It takes fews seconds to apply. Dont miss this great opportunity.

Apply Here

http://bit.ly/Fg-N10500-Weekly

15:54



FEDERAL GOVERNMENT SURVIVAL FUND
GET UPTO ₦30,000 CASH PRIZE IN THE ONGOING SURVIVAL FUND PROGRAM
survivalfund.online

DON'T MISS ANOTHER FEDERAL GOVERNMENT SURVIVAL FUND GRANT

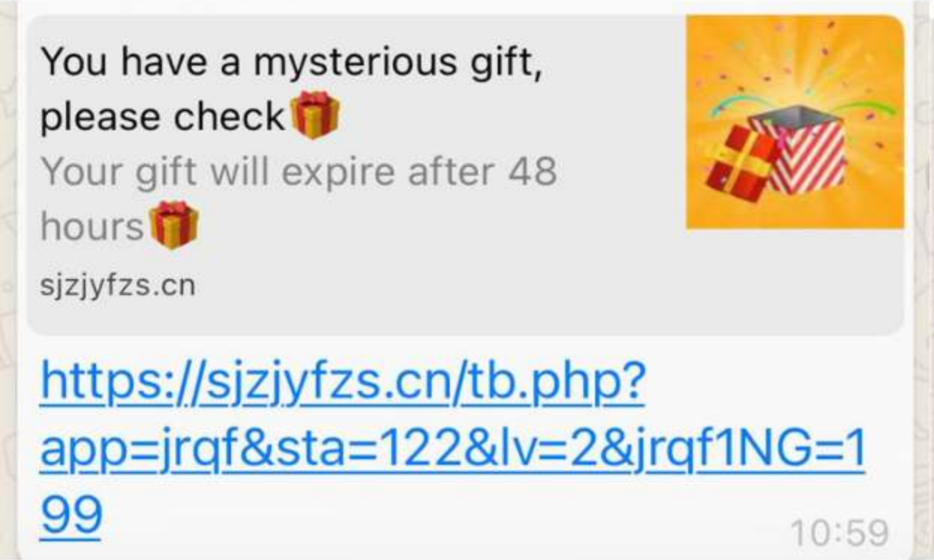
The Federal Government have reopended the Survival Fund Portal
Check if You are Eligible to receive ₦30,000
As Part of SURVIVAL FUND GRANT

Click https://survivalfund.online/CBN/

Oya another one don show.
FG go hear am hard hard.
This guys won't just give up so easily

16:31

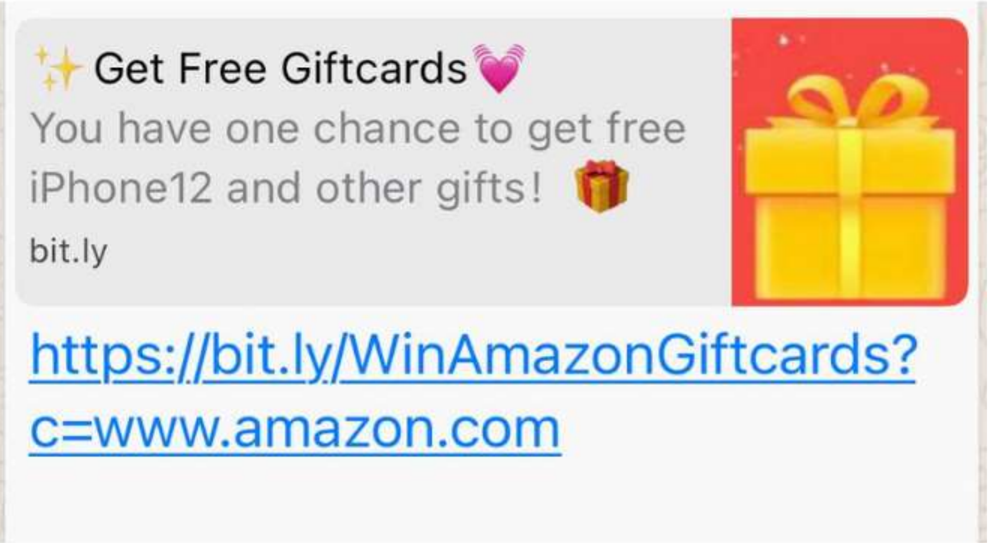
An initiative of cybersafe. FOUNDATION



You have a mysterious gift, please check🎁
Your gift will expire after 48 hours🎁
sjzjyfzs.cn

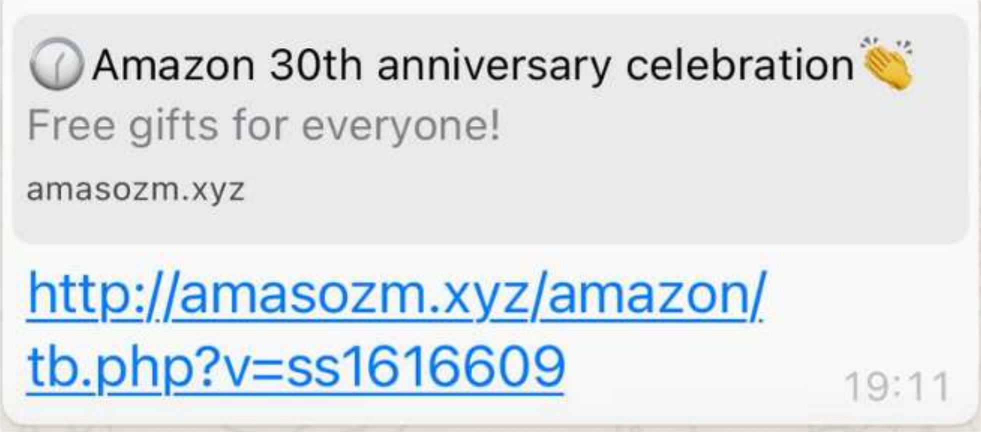
https://sjzjyfzs.cn/tb.php?app=jrqf&sta=122&lv=2&jrqf1NG=199

10:59



✨Get Free Giftcards💓
You have one chance to get free iPhone12 and other gifts! 🎁
bit.ly

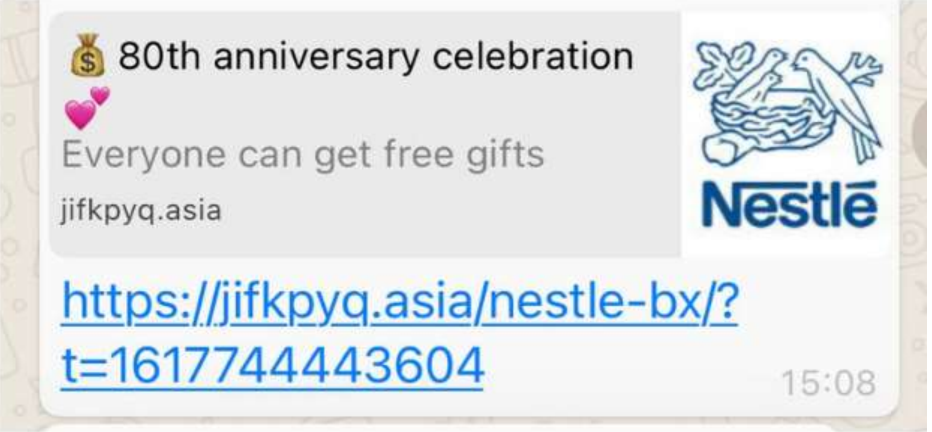
https://bit.ly/WinAmazonGiftcards?c=www.amazon.com



🕐Amazon 30th anniversary celebration👏
Free gifts for everyone!
amasozm.xyz

http://amasozm.xyz/amazon/tb.php?v=ss1616609

19:11



💰 80th anniversary celebration 💕
Everyone can get free gifts
jifkpyq.asia

https://jifkpyq.asia/nestle-bx/?t=1617744443604

15:08

UKaid
from the British people

DigiGirls

THANK YOU

An initiative of
cybersafe.
FOUNDATION

UKaid
from the British people

DigiGirls

SOCIAL ENGINEERING METHODS

An initiative of
cybersafe.
FOUNDATION

UKaid
from the British people

DigiGirls

Social Engineering Methods

- Phishing & Spotting Phishing
- Phishing Types
- Other Social Engineering Methods
- Impact of Social Engineering

An initiative of cybersafe. FOUNDATION

UKaid
from the British people

DigiGirls

Phishing & Spotting Phishing Emails

An initiative of
cybersafe.
FOUNDATION

UKaid
from the British people

DigiGirls

Social Engineering Tricks

- Gaining trust by providing some information- familiar nature (rapport building)
- Helpfulness (presents a problem then becomes the saviour)
- Steer emotions
- Offering rewards
- Urgency
- Stirs fear
- Unrealistic threat or consequence
- Asks you to break protocol

An initiative of
cybersafe.
FOUNDATION

Phishing

Phishing is deception through email which aims to get victims to reveal sensitive information, click on harmful links or open attachments that contain harmful software by disguising as a trustworthy entity in an email.

How to Spot Phishing Emails

- Generic greetings
- Spelling & grammatical errors
- They induce extreme emotions
- Dangerous file attachments
- Contains offers that are too good to be true
- Misspelt domain name
- Malicious links
- Inconsistencies in email address, links and domain names
- Requests for sensitive information.

An initiative of cybersafe. FOUNDATION

UKaid
from the British people

DigiGirls

Can you detect a phishing mail?

Take This Quiz

https://phishingquiz.withgoogle.com/

An initiative of
cybersafe.
FOUNDATION

UKaid
from the British people

DigiGirls

THANK YOU

An initiative of
cybersafe.
FOUNDATION

UKaid
from the British people

DigiGirls

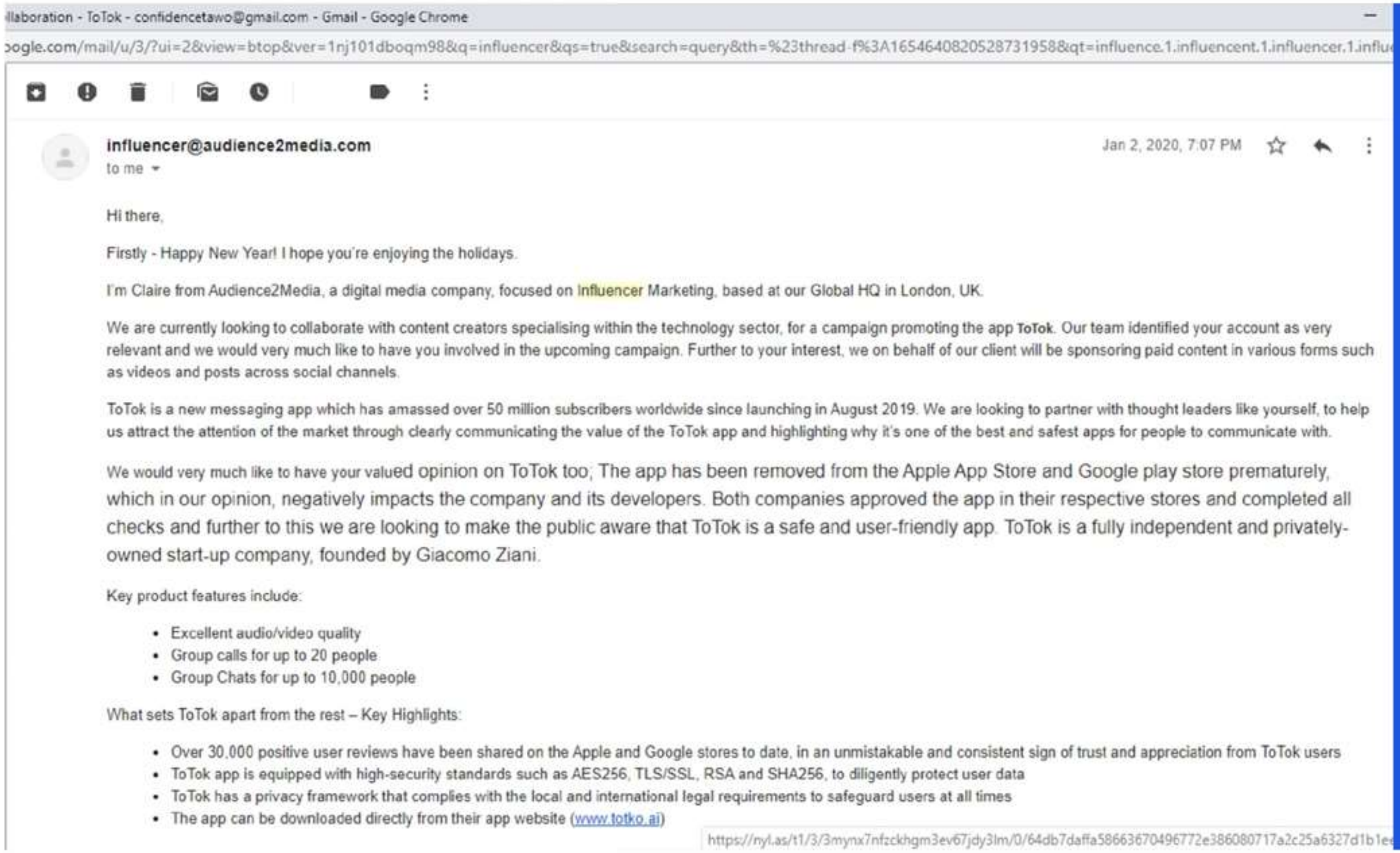
Phishing Types

An initiative of
cybersafe.
FOUNDATION

UKaid
from the British people

Spear Phishing

DigiGirls



llaboration - ToTok - confidencetawo@gmail.com - Gmail - Google Chrome

oogle.com/mail/u/3/?ui=2&view=btop&ver=1nj101dboqm98&q=influencer&qs=true&search=query&th=%23thread-f%3A1654640820528731958&qt=influence.1.influencent.1.influencer.1.influ

influencer@audience2media.com
to me

Jan 2, 2020, 7:07 PM

Hi there,

Firstly - Happy New Year! I hope you're enjoying the holidays.

I'm Claire from Audience2Media, a digital media company, focused on Influencer Marketing, based at our Global HQ in London, UK.

We are currently looking to collaborate with content creators specialising within the technology sector, for a campaign promoting the app ToTok. Our team identified your account as very relevant and we would very much like to have you involved in the upcoming campaign. Further to your interest, we on behalf of our client will be sponsoring paid content in various forms such as videos and posts across social channels.

ToTok is a new messaging app which has amassed over 50 million subscribers worldwide since launching in August 2019. We are looking to partner with thought leaders like yourself, to help us attract the attention of the market through clearly communicating the value of the ToTok app and highlighting why it's one of the best and safest apps for people to communicate with.

We would very much like to have your valued opinion on ToTok too; The app has been removed from the Apple App Store and Google play store prematurely, which in our opinion, negatively impacts the company and its developers. Both companies approved the app in their respective stores and completed all checks and further to this we are looking to make the public aware that ToTok is a safe and user-friendly app. ToTok is a fully independent and privately-owned start-up company, founded by Giacomo Ziani.

Key product features include:

- Excellent audio/video quality
- Group calls for up to 20 people
- Group Chats for up to 10,000 people

What sets ToTok apart from the rest – Key Highlights:

- Over 30,000 positive user reviews have been shared on the Apple and Google stores to date, in an unmistakable and consistent sign of trust and appreciation from ToTok users
- ToTok app is equipped with high-security standards such as AES256, TLS/SSL, RSA and SHA256, to diligently protect user data
- ToTok has a privacy framework that complies with the local and international legal requirements to safeguard users at all times
- The app can be downloaded directly from their app website (www.totko.ai)

https://nyl.as/t1/3/3mynx7nfzckhgm3ev67jdy3lm/0/64db7daffa58663670496772e386080717a2c25a6327d1b1ee

A more targeted version of the phishing scam whereby an attacker chooses specific individuals within an organization. They then tailor their messages based on characteristics, job positions, and contacts belonging to their victims to make their attack less conspicuous.

An initiative of
cybersafe.
FOUNDATION

Vishing

Often referred to as voice phishing, vishing is a deception method cybercriminals use savvy deceptive tactics to convince victims to act, giving up private information and access to bank accounts.

An initiative of cybersafe. FOUNDATION

YOUR BANK, WILL NEVER ASK FOR YOUR PIN, CVV, COMPLETE CARD NUMBER, VERIFICATION CODE OR ONE TIME PASSWORD

Vishing

Smishing is a social engineering attack carried out over mobile text messaging, also known as SMS phishing. Victims are deceived into giving sensitive information to a disguised attacker. It occurs on many mobile text messaging platforms, including non-SMS channels like data-based mobile messaging apps like WhatsApp.

UKaid
from the British people

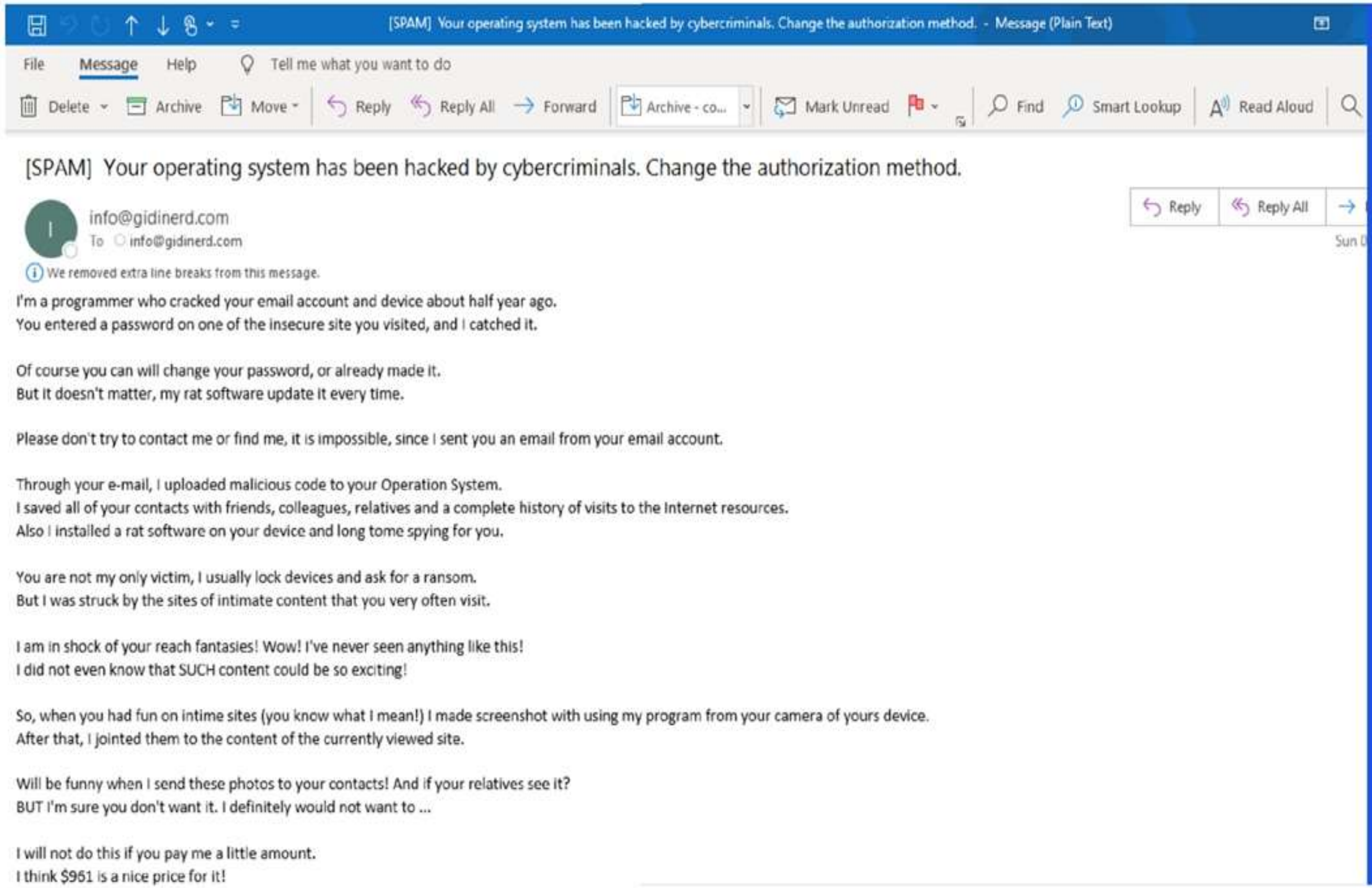
DigiGirls

THANK YOU

An initiative of
cybersafe.
FOUNDATION

Other Social Engineering Methods

Pretexting


[SPAM] Your operating system has been hacked by cybercriminals. Change the authorization method. - Message (Plain Text)
File
Message
Help
Tell me what you want to do
Delete
Archive
Move
Reply
Reply All
Forward
Archive - co...
Mark Unread
Find
Smart Lookup
Read Aloud
Reply
Reply All
Sun

[SPAM] Your operating system has been hacked by cybercriminals. Change the authorization method.

info@gidinerd.com
To info@gidinerd.com

We removed extra line breaks from this message.

I'm a programmer who cracked your email account and device about half year ago.
You entered a password on one of the insecure site you visited, and I catched it.

Of course you can will change your password, or already made it.
But it doesn't matter, my rat software update it every time.

Please don't try to contact me or find me, it is impossible, since I sent you an email from your email account.

Through your e-mail, I uploaded malicious code to your Operation System.
I saved all of your contacts with friends, colleagues, relatives and a complete history of visits to the Internet resources.
Also I installed a rat software on your device and long tome spying for you.

You are not my only victim, I usually lock devices and ask for a ransom.
But I was struck by the sites of intimate content that you very often visit.

I am in shock of your reach fantasies! Wow! I've never seen anything like this!
I did not even know that SUCH content could be so exciting!

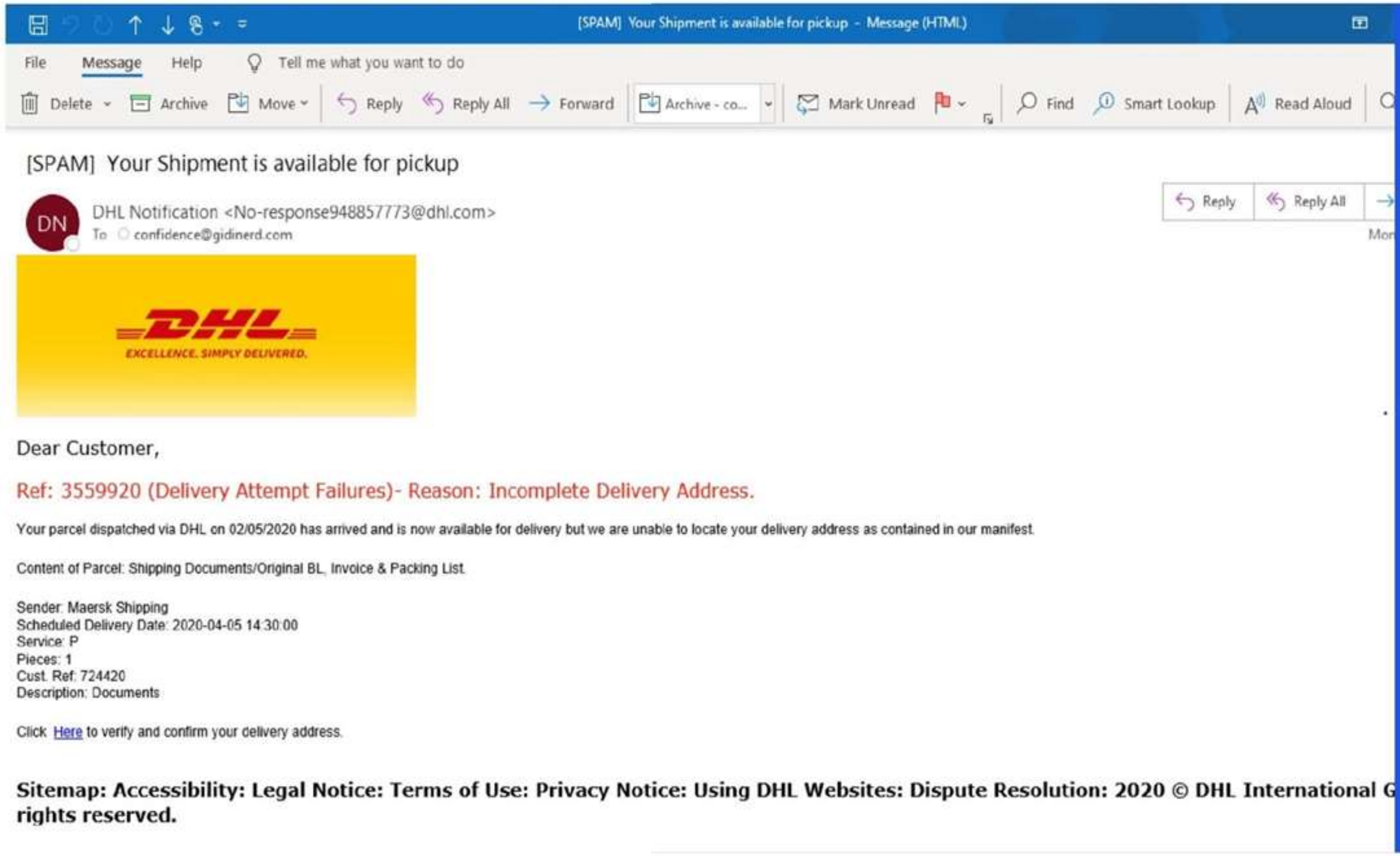
So, when you had fun on intime sites (you know what I mean!) I made screenshot with using my program from your camera of yours device.
After that, I jointed them to the content of the currently viewed site.

Will be funny when I send these photos to your contacts! And if your relatives see it?
BUT I'm sure you don't want it. I definitely would not want to ...

I will not do this if you pay me a little amount.
I think $961 is a nice price for it!

Someone pretends to need sensitive information from you for an alleged critical task.

Spoofing



[SPAM] Your Shipment is available for pickup

DHL Notification <No-response948857773@dhl.com>
To confidence@gidinerd.com

Dear Customer,

Ref: 3559920 (Delivery Attempt Failures)- Reason: Incomplete Delivery Address.

Your parcel dispatched via DHL on 02/05/2020 has arrived and is now available for delivery but we are unable to locate your delivery address as contained in our manifest.

Content of Parcel: Shipping Documents/Original BL, Invoice & Packing List.

Sender: Maersk Shipping
Scheduled Delivery Date: 2020-04-05 14:30:00
Service: P
Pieces: 1
Cust. Ref: 724420
Description: Documents

Click Here to verify and confirm your delivery address.

Sitemap: Accessibility: Legal Notice: Terms of Use: Privacy Notice: Using DHL Websites: Dispute Resolution: 2020 © DHL International G rights reserved.

Pretending to be someone you are not

An initiative of cybersafe. FOUNDATION

UKaid
from the British people

DigiGirls

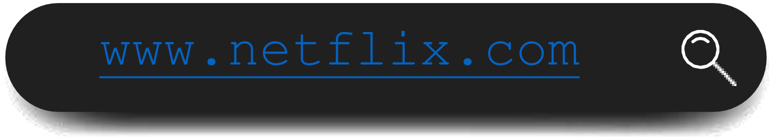
Baiting

Baiting involves luring an unsuspecting victim with a highly attractive offer playing on fear, greed and temptation to make them part with their personal sensitive data like log-in details. Through fraudulent, fake methods, both attempt to capture confidential, personal details such as a password or banking information such as a PIN so they can access your business networks and systems to instal malware which executes ransomware.

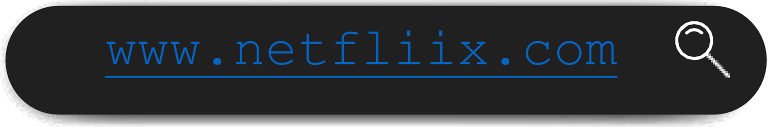
An initiative of
cybersafe.
FOUNDATION

Topic Activity

Spot the difference



www.netflix.com



www.netfliix.com

An initiative of cybersafe. FOUNDATION

UKaid
from the British people

DigiGirls

Topic Activity

Spot the difference

www.npower-fp-fund.gq

www.npower.org

An initiative of
cybersafe.
FOUNDATION

THANK YOU

UKaid
from the British people

DigiGirls

Impact of Social Engineering

An initiative of cybersafe. FOUNDATION

Business Email Compromise

This a social engineering method that targets companies who conduct wire transfers and have suppliers abroad. Corporate or publicly available email accounts of executives or high-level employees related to finance or involved with wire transfer payments are either spoofed or compromised through keyloggers or phishing attacks to do fraudulent transfers, resulting in massive losses.

Business Email Compromise

An impersonation attack typically involves an email that seems to come from a trusted source. like the CEO, CFO or another high-level executive, a trusted colleague, a third-party vendor or other well-known Internet brands requesting you to perform certain financial transactions.

Preventing Business Email Compromise

- Process information and determine truth
- Be wary of tempting offers
- Trust but verify: Multi-channel request verification
- Manually type out web addresses. Make a habit not to click links in emails.
- Review sender's email address
- Scan attachments for malware
- Keep your antivirus/antimalware software updated
- Use multi-factor authentication
- Build a culture of not circumventing due process
- Ensure vendor security

Social Engineering Trends

- Use of shortened URLs
- Combination of Smishing and Vishing
- Baiting with relevance e.g. using seasonal celebration, global events, trending announcements, etc.
- Impersonation
- Targeted emails (Spear phishing)
- Lookalike domains and websites
- Adware/banking malware e.g. trojans
- Opportunity scams
- Investment Scams
- Sponsored social media ads

UKaid
from the British people

DigiGirls

How To Stay Safe

- Stop and think
- Verify authenticity
- Assess – senders name
- Zero trust mindset
- Scan links in emails or attachment
- Turn on 2FA and have a strong password
- Download apps only from your app store
- Have an antivirus installed

An initiative of
cybersafe.
FOUNDATION

UKaid
from the British people

DigiGirls

Activity Break

Do this if that email contains a link or attachment

https://virustotal.com/

An initiative of
cybersafe.
FOUNDATION

UKaid
from the British people

DigiGirls

THANK YOU

An initiative of
cybersafe.
FOUNDATION

UKaid
from the British people

DigiGirls

CYBER FRAUD

An initiative of
cybersafe.
FOUNDATION

Cyber Fraud

Cyber Fraud and Types

Types of Cyber Fraud Part 2

Types of Cyber Fraud Part 3

Cyber Fraud Preventive Measures

UKaid from the British people

An initiative of cybersafe. FOUNDATION

DigiGirls

UKaid
from the British people

DigiGirls

Cyber Fraud and Types

An initiative of
cybersafe.
FOUNDATION

What is Cyber fraud?

Cyber fraud is the use of internet services and a computing device by cybercriminals to defraud another individual, gain access to a victims' personal identity, corrupt their personal and financial information stored online or otherwise take advantage of them.

Cyber fraud is the most common type of fraud and the extensive and popular use of internet banking and mobile banking means there are more opportunities than ever for criminals to commit cyber fraud.

Types of Cyber Fraud

Frequent instances of cyber fraud include;

- Business Fraud
- Credit Card Fraud
- Internet Auction Fraud
- Investment Schemes
- Nigerian Letter Fraud
- Cryptojacking
- Identity Theft
- Software Piracy
- Cyberespionage
- Cyberextortion
- Exit Scam
- Non-delivery Of Merchandise

An initiative of cybersafe. FOUNDATION

Types of Cyber Fraud

Business Fraud

Business fraud consists of dishonest and illegal activities perpetrated by individuals or companies in order to provide an advantageous financial outcome to those persons or establishments. Also known as corporate fraud, these schemes often appear under the guise of legitimate business practices. An array of crimes fall under business fraud, including the following:

- **Charity fraud:** Using deception to get money from individuals believing they are making donations to legitimate charity organizations, especially charities representing victims of natural disasters shortly after the incident occurs.
- **Internet auction fraud:** A fraudulent transaction or exchange that occurs in the context of an online auction site.

Types of Cyber Fraud

- **Non-delivery of merchandise:** Fraud occurring when a payment is sent but the goods and services ordered are never received.
- **Non-payment of funds:** Fraud occurring when goods and services are shipped or rendered but payment for them is never received.
- **Overpayment scheme:** An individual is sent a payment significantly higher than an owed amount and is instructed to deposit the money in their bank account and wire transfer the excess funds back to the bank of the individual or company that sent it. The sender's bank is usually located overseas, in Eastern Europe for example, and the initial payment is found to be fraudulent, often after the wire transfer has occurred.
- **Re-shipping scheme:** An individual is recruited to receive merchandise at their place of residence and subsequently repackage the items for shipment, usually abroad. Unbeknownst to them, the merchandise was purchased with fraudulent credit cards, often opened in their name.

UKaid
from the British people

DigiGirls

THANK YOU

An initiative of
cybersafe.
FOUNDATION

UKaid
from the British people

DigiGirls

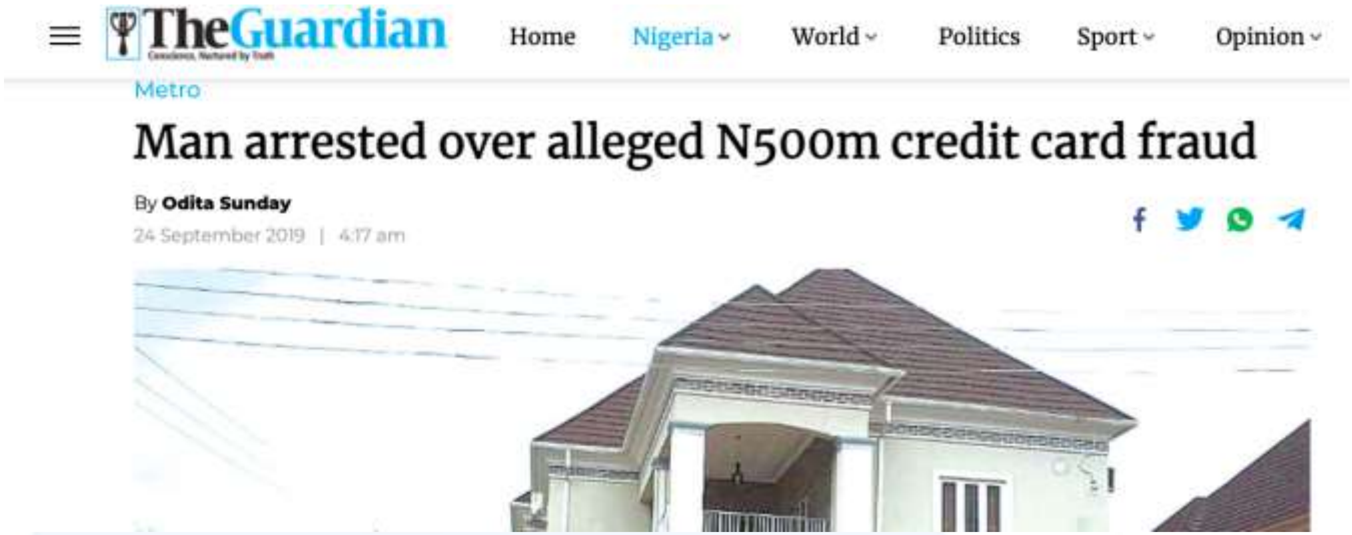
Types of Cyber Fraud
Part 2

An initiative of
cybersafe.
FOUNDATION

Types of Cyber Fraud

Credit Card Fraud

Credit card fraud is the unauthorized use of a credit or debit card, or similar payment tool (ACH, EFT, recurring charge, etc.), to fraudulently obtain money or property. Credit and debit card numbers can be stolen from unsecured websites or can be obtained in an identity theft scheme.



Metro

Man arrested over alleged N500m credit card fraud

By Odita Sunday

24 September 2019 | 4:17 am

Types of Cyber Fraud

Internet Auction Fraud

Internet auction fraud involves schemes attributable to the misrepresentation of a product advertised for sale through an Internet auction site or the non-delivery of products purchased through an Internet auction site.

Non-delivery of Merchandise

Non-delivery of merchandise is a scheme most often linked to Internet auction fraud, in which a seller on an Internet auction website accepts payment for an item yet intentionally fails to ship it. Sellers like these sometimes will relist the item and attempt to sell it again through a different username. Non-delivery of merchandise can also be considered a form of business fraud in a number of cases.

Types of Cyber Fraud

Investment Fraud

Investment fraud involves the illegal sale or purported sale of financial instruments. The typical investment fraud schemes are characterized by offers of low- or no-risk investments, guaranteed returns, overly-consistent returns, complex strategies, or unregistered securities. Examples of investment fraud include advance fee fraud, Ponzi schemes, pyramid schemes, and market manipulation fraud.

These schemes often seek to victimize affinity groups—such as groups with a common religion or ethnicity—to utilize the common interests to build trust to effectively operate the investment fraud against them. The perpetrators range from professional investment advisers to persons trusted and interacted with daily, such as a neighbor or sports coach.

Types of Cyber Fraud

Nigerian Letter Frauds

Nigerian letter frauds combine the threat of impersonation fraud with a variation of an advance fee scheme in which a letter mailed, or e-mailed, from Nigeria offers the recipient the “opportunity” to share in a percentage of millions of dollars that the author—a self-proclaimed government official—is trying to transfer illegally out of Nigeria. The recipient is encouraged to send information to the author, such as blank letterhead stationery, bank name and account numbers, and other identifying information using a fax number given in the letter or return e-mail address provided in the message. The scheme relies on convincing a willing victim, who has demonstrated a “propensity for larceny” by responding to the invitation, to send money to the author of the letter in Nigeria in several instalments of increasing amounts for a variety of reasons.

THANK YOU

UKaid
from the British people

DigiGirls

An initiative of
cybersafe.
FOUNDATION

UKaid
from the British people

DigiGirls

Types of Cyber Fraud Part 3

An initiative of
cybersafe.
FOUNDATION

Types of Cyber Fraud

Cryptojacking

Cryptojacking is a type of cybercrime that involves the unauthorized use of people's devices (computers, smartphones, tablets, or even servers) by cybercriminals to mine for cryptocurrency. Like many forms of cybercrime, the motive is profit, but unlike other threats, it is designed to stay completely hidden from the victim.

Identity Theft

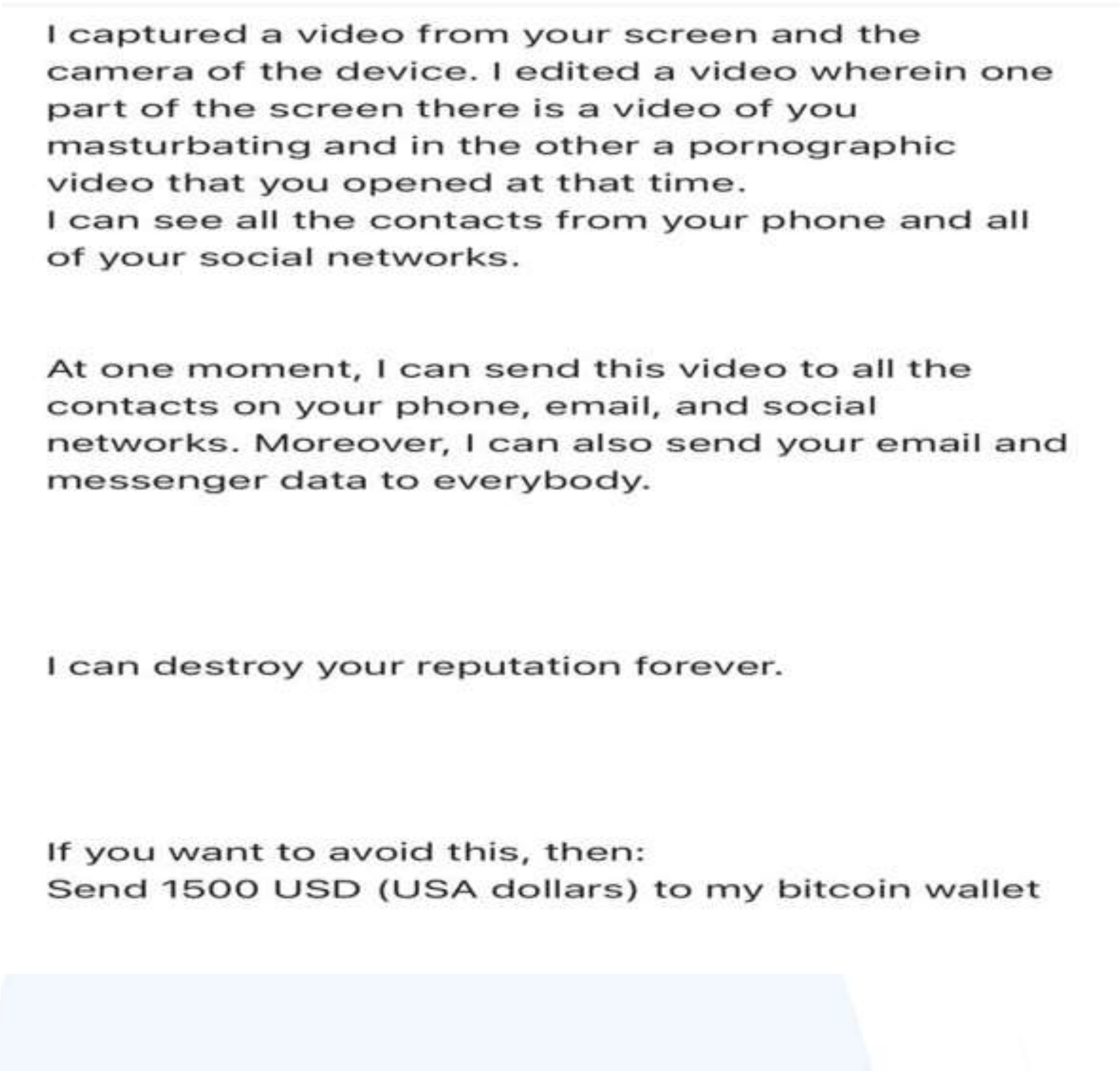
Identity theft and identity fraud are terms used to refer to all types of crime in which someone wrongfully obtains and uses another person's personal data in some way that involves fraud or deception, typically for economic gain.

Types of Cyber Fraud

Cyber Extortion

Cyber extortion is the act of cyber-criminals demanding payment through the use of or threat of some form of malicious activity against a victim, such as data compromise or denial of service attack. Cyber extortion permeates actions such as ransomware, email ransom campaigns, and distributed denial of service (DDoS) attacks.

Types of Cyber Fraud



I captured a video from your screen and the camera of the device. I edited a video wherein one part of the screen there is a video of you masturbating and in the other a pornographic video that you opened at that time.
I can see all the contacts from your phone and all of your social networks.

At one moment, I can send this video to all the contacts on your phone, email, and social networks. Moreover, I can also send your email and messenger data to everybody.

I can destroy your reputation forever.

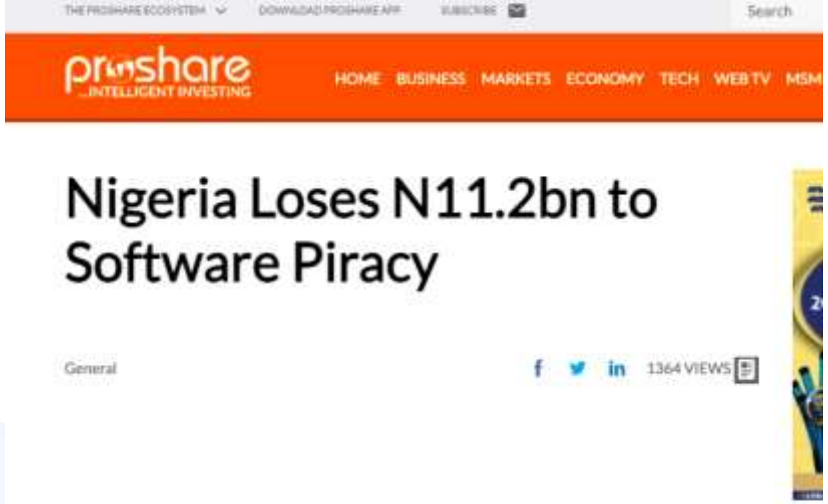
If you want to avoid this, then:
Send 1500 USD (USA dollars) to my bitcoin wallet

An initiative of cybersafe. FOUNDATION

Types of Cyber Fraud

Software Piracy

Software piracy is the illegal copying, installation, use, distribution, or sale of software in any way other than that is expressed in the license agreement. The software industry is facing huge financial losses due to the piracy of software. Piracy of software is performed by end-users as well as by the dealers.



Nigeria Loses N11.2bn to Software Piracy

General

1364 VIEWS

Types of Cyber Fraud

Exit Scam

An exit scam is a confidence trick where an established business stops shipping orders while receiving payment for new orders. If the entity had a good reputation, it could take some time before it is widely recognized that orders are not shipping, and the entity can then make off with the money paid for unshipped orders.

Cyberespionage

Cyber espionage, or cyber spying, is a type of cyberattack in which an unauthorized user attempts to access sensitive or classified data or intellectual property (IP) for economic gain, competitive advantage or political reasons.

Types of Cyber Fraud

Exit Scam

An exit scam is a confidence trick where an established business stops shipping orders while receiving payment for new orders. If the entity had a good reputation, it could take some time before it is widely recognized that orders are not shipping, and the entity can then make off with the money paid for unshipped orders.

Cyberespionage

Cyber espionage, or cyber spying, is a type of cyberattack in which an unauthorized user attempts to access sensitive or classified data or intellectual property (IP) for economic gain, competitive advantage or political reasons.

UKaid
from the British people

DigiGirls

THANK YOU

An initiative of
cybersafe.
FOUNDATION

UKaid
from the British people

DigiGirls

Cyber Fraud Preventive Measures

An initiative of
cybersafe.
FOUNDATION

How to Prevent Cyber Fraud

- Continually update your computer and mobile devices.
- Use good password habits
- Restrict access to your computer and devices by using passwords and multiple computer profiles
- Talk to your children and family about internet security.
- Know what to do if you become a victim.
- Activate your firewall – Firewalls are the first line of cyber defence; they block connections to unknown or bogus sites and will keep out some types of viruses and hackers.
- Use anti-virus/malware software - Prevent viruses from infecting your computer by installing and regularly updating anti-virus software.

How to Prevent Cyber Fraud

- Prevent spyware from infiltrating your computer by installing and updating anti-spyware software.
- Check your security settings and be careful what information you post online.
- Be aware that your mobile device is vulnerable to viruses and hackers.
- Be aware that your mobile device is vulnerable to viruses and hackers.
- Download applications from trusted sources. Install the latest operating system updates Keep your applications and operating system (e.g. Windows, Mac, Linux) current with the latest system updates.
- Turn on automatic updates to prevent potential attacks on older software.
- Make regular back-ups of all your important data, and store it in another location.

How to Prevent Cyber Fraud

- Secure your wireless network. Wi-Fi (wireless) networks are vulnerable to intrusion if they are not properly secured
- Review and modify default settings.
- Public Wi-Fi, a.k.a. "Hot Spots", are also vulnerable. Avoid conducting financial or corporate transactions on these networks.
- Be cautious when giving out personal information such as your name, address, phone number or financial information on the Internet.

How to Prevent Cyber Fraud

- Make sure that websites are secure (e.g. when making online purchases) or that you've enabled privacy settings (e.g. when accessing/using social networking sites).
- Always think before you click on a link or file of unknown origin.
- Don't feel pressured by any emails. Check the source of the message. When in doubt, verify the source.
- Never reply to emails that ask you to verify your information or confirm your user ID or password.

UKaid
from the British people

DigiGirls

THANK YOU

An initiative of
cybersafe.
FOUNDATION

UKaid
from the British people

DigiGirls

Protecting Against Viruses and Other Malwares

An initiative of
cybersafe.
FOUNDATION

Malware

CONTENT

- What is Malware?
- Types of Malwares
- Case Studies
- Signs of a Malware Attack
- Preventive Measures

Malware Case Study

UKaid
from the British people

DigiGirls

An initiative of
cybersafe.
FOUNDATION

What is a Malware?

Malware is shorthand for malicious software. Malware is a collective name for a number of malicious software variants, including viruses, ransomware and spyware. This software is intentionally designed to cause damages to a computer, server, client or computer network.

Types of Malware

- Viruses
- Trojan
- Worms
- Rootkit
- Key loggers
- Ransomeware
- Adware
- Spyware

Case Study 1

https://thehackernews.com/2023/03/nexus-new-rising-android-banking-trojan.html

An initiative of cybersafe. FOUNDATION

Case Study 2

https://vpnoverview.com/news/nigerian-hacker-solicits-disgruntled-employees-and-accidently-reveals-his-identity/

Case Study 3

https://www.kaspersky.com/about/press-releases/2023_industrial-sector-attacks-on-the-rise-an-annual-overview-by-kaspersky

Case Study 4

https://www.bleepingcomputer.com/news/security/new-hook-android-malware-lets-hackers-remotely-control-your-phone/#:~:text=A%20new%20Android%20malware%20named,VNC%20(virtual%20network%20computing).

An initiative of cybersafe. FOUNDATION

UKaid
from the British people

DigiGirls

THANK YOU

An initiative of
cybersafe.
FOUNDATION

UKaid
from the British people

DigiGirls

Malware Types Part 1

An initiative of
cybersafe.
FOUNDATION

Business Email Compromise

This a social engineering method that targets companies who conduct wire transfers and have suppliers abroad. Corporate or publicly available email accounts of executives or high-level employees related to finance or involved with wire transfer payments are either spoofed or compromised through keyloggers or phishing attacks to do fraudulent transfers, resulting in massive losses.

Viruses

A computer virus is a type of malicious code or program written to alter the way a computer operates and is designed to spread from one computer to another.

A virus operates by inserting or attaching itself to a legitimate program or document that supports macros in order to execute its code.

Worms

Worms are basically harmful software which uses network/system vulnerabilities to spread themselves from system to system. They are typically part of other software such as rootkits and are normally the entry point into the system. They basically compromise the system (locally or remotely) and provide access to other malware.

Rootkit

A rootkit is a clandestine computer program designed to provide continued privileged access to a computer while actively hiding its presence. Originally, a rootkit was a collection of tools that enabled administrator-level access to a computer or network.

Root refers to the Admin account on Unix and Linux systems, and kit refers to the software components that implement the tool.

Ransomware

Ransomware is a form of malware that encrypts a victim's files. The attacker then demands a ransom from the victim to restore access to the data upon payment.

Users are shown instructions for how to pay a fee to get the decryption key. The costs can range from a few hundred dollars to thousands, payable to cybercriminals in Bitcoin.

Trojans

Trojan is a type of malware that invade your computer disguised as a real, operational programs. Once a trojan is inside your system, it can perform destructive actions before you even know it’s there. Once inside, some trojans sit idly on your computer and wait for further instructions from its host hacker, but others begin their malicious activity right from the start.

UKaid
from the British people

DigiGirls

THANK YOU

An initiative of
cybersafe.
FOUNDATION

UKaid
from the British people

DigiGirls

Malware Types Part 2

An initiative of
cybersafe.
FOUNDATION

Spyware

Spyware is loosely defined as malicious software designed to enter your computer device, gather data about you, and forward it to a third-party without your consent. Spyware can also refer to legitimate software that monitors your data for commercial purposes like advertising. However, malicious spyware is explicitly used to profit from stolen data.

Keyloggers

A keylogger is an insidious form of spyware. You enter sensitive data onto your keyboard, believing nobody is watching. In fact, keylogging software is hard at work logging everything that you type.

Adware

Adware, also known as advertisement-supported software, is software that displays unwanted (and sometimes irritating) pop-up adverts which can appear on your computer or mobile device. It generates revenue for its developers by automatically generating adverts on your screen, usually within a web browser.

Scareware

Scareware is a social engineering tactic that manipulates users into believing they need to download or buy malicious, sometimes useless, software. Most often initiated using a pop-up ad. Scareware uses social engineering to take advantage of a user's fear, coaxing them into installing fake anti-virus software.

UKaid
from the British people

DigiGirls

THANK YOU

An initiative of
cybersafe.
FOUNDATION

UKaid
from the British people

DigiGirls

Signs of a Malware Attack

An initiative of
cybersafe.
FOUNDATION

Signs of a Malware Attack

- Frequent pop-up windows.
- Your usual homepage may change to another website, for instance. Plus, you may be unable to reset it.
- Mass emails being sent from your email account.
- Frequent system crashes.
- Unusually slow computer performance.
- Unknown programs that start up when you turn on your computer.

Signs of a Malware Attack

- Unusual activities like password changes. This could prevent you from logging into your computer.
- Unusually slow or frozen system functionality
- Spam and pop-up ads
- Unknown icons on the desktop
- Redirection from a popular website to an unknown one
- New files or folders created without your permission

THANK YOU

UKaid
from the British people

DigiGirls

How Malware Spreads

An initiative of
cybersafe.
FOUNDATION

How Malware Spreads

Malware is typically distributed via:

1. Email attachments
2. Infected external storage devices
3. Fake internet ads
4. Social engineering tactics
5. Infected applications or websites

How Malware Spreads

Often, users are tricked into downloading malware with links or pop-ups that seem legitimate such as:

- Flashing messages like, “Your computer has been infected! Click here to run a scan!”
- Unknown applications that purport to convert files, unzip files or find discounts
- “Gifts” or “prizes” offered for clicking a button
- Clicking the link or button directs the user to a website that automatically installs malware onto their computer.

UKaid
from the British people

DigiGirls

THANK YOU

An initiative of
cybersafe.
FOUNDATION

UKaid
from the British people

DigiGirls

Malware Preventive Measures

An initiative of
cybersafe.
FOUNDATION

UKaid
from the British people

DigiGirls

Preventive Measures

- Keep your computer and software updated
- Think twice before clicking links or downloading anything
- Be careful about opening email attachments or images
- Don't trust pop-up windows that ask you to download software
- Limit your file sharing
- Use an antivirus software

UKaid
from the British people

DigiGirls

Preventive Measures

- Only buy Apps from trusted sources
- Install a firewall
- Back up your data regularly
- Get a password manager
- Only access secured sites
- Read emails with an eagle eye.

An initiative of
cybersafe.
FOUNDATION

UKaid
from the British people

DigiGirls

Topic Activity

- Scan malicious links or attachments using VirusTotal
- Find a case study of a cyber attack and identify what malware variants were used

An initiative of
cybersafe.
FOUNDATION

THANK YOU

Keeping Your Smartphones, Tablets and Computers Safe

An initiative of cybersafe. FOUNDATION

Content

Data Protection

Secure settings for your computer and mobile devices

Device Security

Safe software download and installation

Secure Remote Working

UKaid from the British people

DigiGirls

An initiative of cybersafe. FOUNDATION

Data Protection

Data Protection

Data protection is the process of safeguarding important information from corruption, compromise or loss.

Data protection is a set of strategies and processes you can use to secure the privacy, availability, and integrity of your data. It is sometimes also called data security or information privacy.

CASE STUDY

https://nation.africa/kenya/business/mobile-lenders-ditch-debt-collectors-to-escape-sting-of-debt-shaming-law-4096420

UKaid
from the British people

DigiGirls

THANK YOU

An initiative of
cybersafe.
FOUNDATION

UKaid
from the British people

DigiGirls

Secure settings for your computer and mobile devices

An initiative of
cybersafe.
FOUNDATION

Tip 1: Switch on password protection

Devices such as mobile phones, computers and tablets are commonly used for work to send and receive business emails and sharing of sensitive information which makes these devices a target by hackers trying to steal the information for their personal gain.

- By enabling password protection on your device this will prevent unauthorized users from gaining access to your device and ensure your data remain protected.
- It does not stop at just enabling password protection, it is important to practice a good password hygiene by applying the following:
- Use of Password Manager
- Use a Strong Password
- Enable Two-Factor Authentication (2FA)
- Make Use of Unique Password

Tip 2: Keep your Device up to date

The best ways to protect your device is to ensure it is running the latest update by following these steps:

- Frequently run scans on all your devices to discover missing updates.
- Frequently apply update on your device.

Tip 3: Make sure lost or stolen devices can be tracked, locked or wiped

It is important to enable Mobile Device Management (MDM) on your devices to allow you manage your device remotely in an event it is lost or stolen you can easily track, lock or wipe your data on the device. This removes the risk of your data falling into the wrong hands and the damaging effect it can have on your business.

Tip 4: Install a licensed antivirus

The foundation to having a good security posture is to install antivirus on your device. It is important to have a licensed and properly configured antivirus in your, device to protect you from attacks by bad actors.

Tip 5: Keep apps and software up to date

Vulnerabilities are discovered daily on applications and these vulnerabilities can be exploited by attackers to gain access to your device and steal sensitive information or go to the extreme of damaging your device. Frequently check for software update and apply on your applications to ensure you are protected from zero-day attacks.

Tip 6: Avoid public Wi-Fi hotspot

Using a public Wi-Fi makes you an easy pre for an attacker as they can easily gain access to your device and steal your data. They could also plant a monitoring tool on the network to spy on your internet browsing activities. Unlike a private Wi-Fi most public ones don’t have any form of security in place to protect the users connected to the network.

Tip 7: Leverage built-in Encryption

Encryption helps you protect the data on your disk by converting it into an unreadable format and only becomes readable when the correct password is provided on the encryption software. In the event your device is lost or stolen, the data on the disk cannot be viewed in its readable form.

You can leverage on Microsoft Windows inbuilt encryption “BitLocker” and Apple Mac inbuilt encryption “FileVault” to encrypt your laptop disk.

UKaid
from the British people

DigiGirls

THANK YOU

An initiative of
cybersafe.
FOUNDATION

UKaid
from the British people

DigiGirls

Device Security

An initiative of
cybersafe.
FOUNDATION

Controlling Access to Data

Access control governs the resources that an unauthenticated user is able to read, modify, or write. Access control is a method of guaranteeing that users are who they say they are and that they have the appropriate access to company data.

Access control is a selective restriction of access to data, it consists of two main components:

- **Authentication** is a technique used to verify that someone is who they claim to be. Authentication isn't sufficient by itself to protect data; data protection needs an additional layer.
- **Authorization** determines whether a user should be allowed to access the data or make the transaction they are attempting.

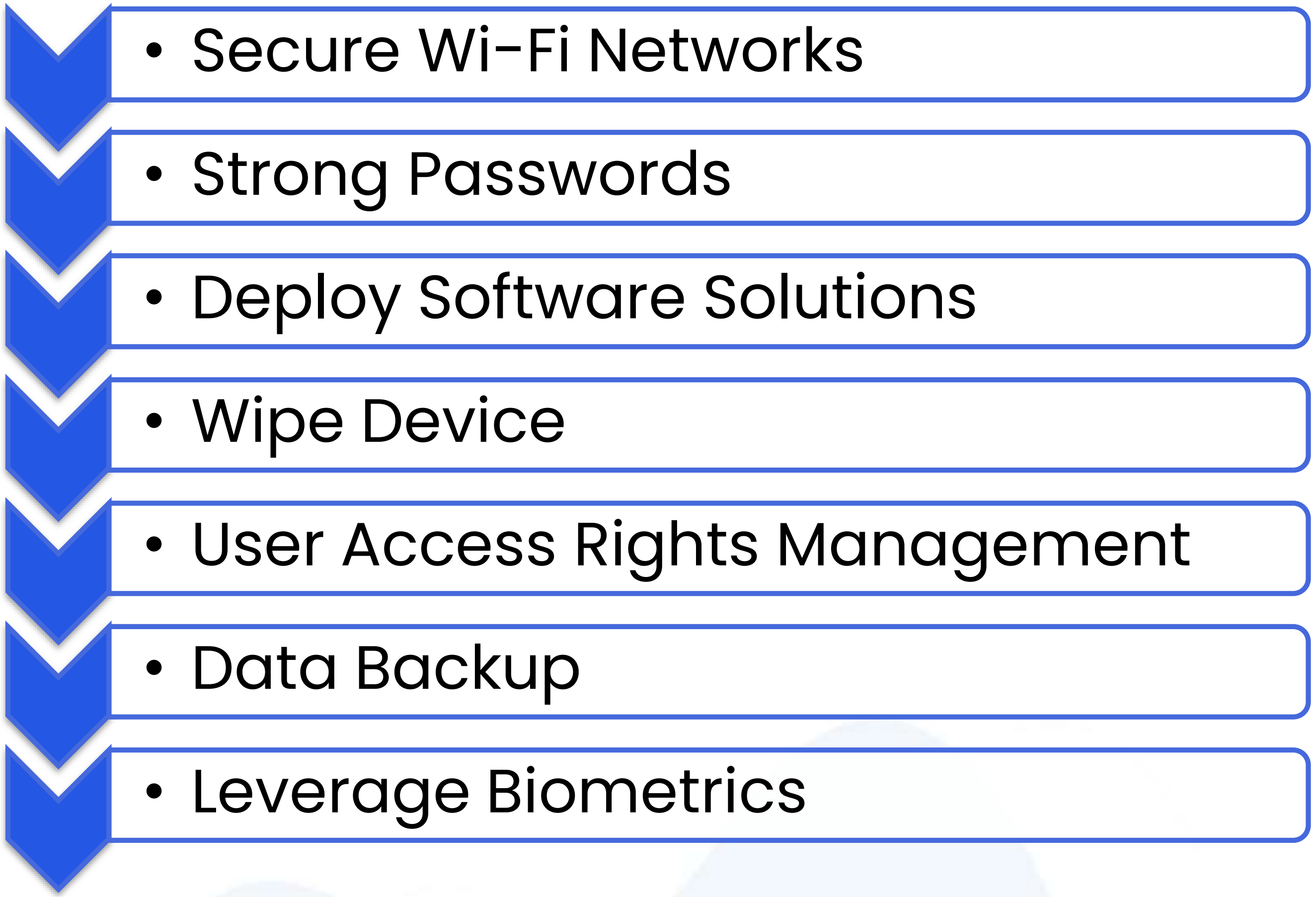
Keeping Your Devices Safe

1. Always use a password
2. Use password manager. Don't write your password on a piece of paper or store on a notepad on your system to prevent it from falling into the wrong hands.
3. Use a strong password. Your password must contain upper case and lower case alphabets, numbers, special characters and much be at least 8 characters long.
4. Use 2factor authentication
5. Use a different password for different accounts
6. Install a licensed antivirus software
7. Keep apps and software up to date

Keeping Your Devices Safe

8. Keep your device up to date. Ensure it is running on the latest updates
    - Frequently run scans on all your devices to discover the missing updates and apply them
    - Subscribe to vendor's security awareness channel to get news updates on newly discovered innovative and software updates
9. Make sure lost or stolen devices can be tracked, locked or wiped. Enable mobile device management on your devices to allow you manage your device remotely.
10. Avoid public Wi-Fi hotspot
11. Leverage built in encryption (e.g., bitlocker and Apple filevault

Device Security Strategies



- Secure Wi-Fi Networks
- Strong Passwords
- Deploy Software Solutions
- Wipe Device
- User Access Rights Management
- Data Backup
- Leverage Biometrics

THANK YOU

UKaid
from the British people

DigiGirls

Safe Software Download and Installation

An initiative of
cybersafe.
FOUNDATION

Safe Software Download and Installation

Tip 1: Avoid Unsolicited Links

The most effective and easiest thing you can do to avoid malware and adware is to avoid downloading any software program or app from an unsolicited link. Avoid downloading anything that you've received a link to via an email, text, or some other personal message unless you completely trust the source.

Safe Software Download and Installation

Tip 4: Free Downloads ≠ Free Software

Free download does not mean that the software is free to use. Before downloading something that is labelled “free” or as a “free download,” check to see that the program description clearly states that it’s freeware or completely free to use.

Tip 5: Avoid Tricky ‘Download’ Ads

Don’t be tricked by “Download” advertisements. These sorts of advertisements run frequently on software download pages, appearing as giant download buttons. These download advertisements usually go to a malware-ridden page where you get to download something else. Not all software download pages have download buttons either, many are just links.

Safe Software Download and Installation

Tip 6: Avoid Installers and Download Managers

One way these download sites make their money is by wrapping the downloads they serve inside of a program called an **installer** or a **download manager**.

These programs are often referred to users as **PUPs** – Potentially Unwanted Programs; these programs have nothing to do with the program you're trying to download and install.

Tip 7: Choose 'Custom Installation'

During downloads, when choose **Custom Installation** when given the option. This option makes the install process a bit longer with the few extra screens it adds, but it's almost always where the "don't install this" options are hidden. One way to avoid installation-based problems is to choose portable software instead of installable software.

UKaid
from the British people

DigiGirls

THANK YOU

An initiative of
cybersafe.
FOUNDATION

UKaid
from the British people

DigiGirls

Secure Remote Working

An initiative of
cybersafe.
FOUNDATION

Best Practices for Working Remotely

- Use antivirus and internet security software at home.
- Secure your home Wi-Fi.
- Make sure your passwords are strong and secure.
- Keep family members away from work devices.
- Avoid public Wi-Fi; if necessary, use personal hotspots or some way to encrypt your web connection.
- Be wary of email scams and your email security.

UKaid
from the British people

DigiGirls

Best Practices for Working Remotely

- Keep work data on work computers.
- Run software updates regularly.
- Use a VPN.
- Encrypt sensitive data in emails and on your device.
- Never leave your bag, briefcase or laptop unattended.
- Don’t use random thumb drives.

An initiative of
cybersafe.
FOUNDATION

UKaid
from the British people

DigiGirls

Browsing the Internet Securely

1. Keep your browser and any plugins updated
2. Use a browser that allows you to take your bookmarks with you in between devices
3. Block Pop-ups
4. Use an ad blocker
5. Use a VPN
6. Use a password manager
7. Ensure you have an up-to-date antivirus and firewall protection
8. Beware of public (unprotected) Wi-Fi
9. Https

An initiative of
cybersafe.
FOUNDATION

UKaid
from the British people

DigiGirls

THANK YOU

An initiative of
cybersafe.
FOUNDATION

UKaid
from the British people

DigiGirls

Keeping Your Online Accounts Secure

An initiative of
cybersafe.
FOUNDATION

UKaid
from the British people

DigiGirls

Content

- Case Study
- Tips to Protect your Social Media and other Online Accounts
- Safe Web Browsing and Best Practices
- Using Passwords to Protect your Data
- Turning on Extra Security

An initiative of
cybersafe.
FOUNDATION

Case Study

https://techcrunch.com/2017/12/22/that-time-i-got-locked-out-of-my-google-account-for-a-month/

Case Study

https://www.cbsnews.com/boston/news/scammers-hack-facebook-accounts-fake-taylor-swift-tickets/

An initiative of cybersafe. FOUNDATION

THANK YOU

UKaid
from the British people

DigiGirls

Tips to Protect your Social Media and Other Online Accounts

An initiative of
cybersafe.
FOUNDATION

Keeping Social Media Accounts Secure

1. Choose a strong password
2. Use a different password for each social media account.
3. Seal it off by adding an extra layer of security with 2factor authentication.
4. Never click on links without ensuring they are safe.
5. Make sure you scan all attachments for viruses before you download them.
6. Limit the amount of information you share online
7. Review privacy settings

Safe Web Browsing

What does the padlock at the top of your browser window really mean?

What websites shouldn’t you be visiting?

An initiative of cybersafe. FOUNDATION

Safe Web Browsing

- Do not leave your device unattended to, if you must, ensure to lock the screen.
- Change your password if you think someone may have learned (seen, heard) it
- Observe a clean desk policy
- Do not share personal or sensitive information on social media
- Be wary of links and attachments in emails

UKaid
from the British people

DigiGirls

THANK YOU

An initiative of
cybersafe.
FOUNDATION

UKaid
from the British people

DigiGirls

Using Passwords to Protect your Data

An initiative of
cybersafe.
FOUNDATION

What is a Password?

A password is a string of characters used to verify the identity of a user during the authentication process. Passwords are typically used in conjuncture with a username; they are designed to be known only to the user and allow that user to gain access to a device, application, or website.

Passwords can vary in length and can contain letters, numbers, and special characters.

Creating A Strong Password

Passwords are gatekeepers to your most important information. Cyber attackers are opportunistic and can easily crack weak password.

Strong passwords are passwords no one can ever guess; not even your loved ones.

A strong password must meet the following criteria:

- Must contain a minimum of one uppercase letter e.g A-Z
- Must contain a minimum of one lowercase letter e.g a-z
- Must contain a digit e.g 0-9
- Must be at least 12-characters long e.g Abcd1234
- Must contain special characters e.g. ~!@#$%^&*()_-+=

Creating A Strong Password

A Strong Password **should not**:

- Spell a word or series of words (that make sense together) that can be found in a dictionary
- Spell a word with a number added to the beginning and the end
- Be based on any personal information such as user id, family name, pet, birthday, etc.
- Be a word you use a lot, your favourite colour, your date of birth, pet names, numbers in sequential order, repeated character or series of characters etc. Common offenders include "123456," "password," “AAAA,” and "qwerty".

Topic Activity

Create a strong password

An initiative of cybersafe. FOUNDATION

UKaid
from the British people

DigiGirls

THANK YOU

An initiative of
cybersafe.
FOUNDATION

UKaid
from the British people

DigiGirls

Techniques For Creating A Memorable Password

An initiative of
cybersafe.
FOUNDATION

Techniques For Creating A Memorable Password

Passphrase Method

A passphrase is a sequence of words or other text used to control access to a computer system, program or data. A passphrase is similar to a password in usage, but it is generally longer for added security.

For example, you might choose the easily memorable phrase, ‘Osapa London at Lekki phase 1’ and make your passphrase ‘osapaLONDON@lekkiphase1’

Techniques For Creating A Memorable Password

Storytelling method

In this method you make a sentence out of something that has happened in your life and string the first alphabets of each word to form a password.

A perfect example is a sentence like “The first time I took a French quiz I scored 99% and won a cash gift of 20 dollars.” So, your password will become this **TftItaFqIs99%awacgo20$**.

This password has 22 characters, is a mixture of numbers, symbols, uppercase and lowercase letters.

UKaid
from the British people

DigiGirls

Topic Activity

Create a password using storytelling method

An initiative of
cybersafe.
FOUNDATION

UKaid
from the British people

DigiGirls

THANK YOU

An initiative of
cybersafe.
FOUNDATION

UKaid
from the British people

DigiGirls

Password Hygiene Best Practices

An initiative of
cybersafe.
FOUNDATION

UKaid
from the British people

Password Hygiene Best Practices

DigiGirls

1. Choose a strong password. Choosing strong passwords are critical as they prevent unauthorized access to your physical devices and online account.
2. Avoid Personal identifiers
3. Change all default passwords
4. Avoid using browsers to create and manage passwords.
5. Where possible ensure it is not a dictionary word.
6. Ensure it is unique per platform.
7. Use a password manager. Some popular password managers include, one password, lastpass, dashlane, sticky passwords etc.
8. Turn on an extra layer of security.

THANK YOU

UKaid
from the British people

DigiGirls

An initiative of
cybersafe.
FOUNDATION

UKaid
from the British people

DigiGirls

Password Manager

An initiative of
cybersafe.
FOUNDATION

Password Manager

A password manager is a computer program that allows users to store, generate, and manage their passwords for local applications and online services.

A password manager assists in generating and retrieving complex passwords, storing such passwords in an encrypted database.

UKaid
from the British people

DigiGirls

Importance of Password Managers

1. Password managers protect you by helping you create strong, unique passwords for every service you use, and removing your need to enter those passwords.
2. Remember Only One Password
3. Password managers can prevent password-reuse attacks.
4. Password managers can prevent impostor websites from “phishing” you.
5. Password managers track which services you have accounts with, helping you identify unused accounts that you may want to close or delete data from to reduce your online exposure.

An initiative of
cybersafe.
FOUNDATION

Importance of Password Managers

6. Most password managers have password generators that help generate strong passwords.
7. You can still use the form autofill feature when you have a password safe. Instead of letting your web browser save your form information, entrust your password manager to store your personal information safely.
8. You can share passwords to joint accounts with family or coworkers. It is generally not recommended you give away your personal passwords, but for shared accounts, a password manager gives you the option to control who has access to passwords.

Topic Activity

Download and setup a password manager

An initiative of cybersafe. FOUNDATION

THANK YOU

UKaid
from the British people

DigiGirls

An initiative of
cybersafe.
FOUNDATION

Extra Layer of Security

UKaid
from the British people

DigiGirls

Extra Layer of Security

Thumbprint

Eye Sanner

Token

Facial Recognition

Voice Recognition

OTP

An initiative of
cybersafe.
FOUNDATION

UKaid
from the British people

DigiGirls

THANK YOU

An initiative of
cybersafe.
FOUNDATION

UKaid
from the British people

DigiGirls

Protecting Against IoT and AI Attacks

An initiative of
cybersafe.
FOUNDATION

Content

- IoT Attacks and Defense
- The Rise of Intelligent Machines

UKaid
from the British people

DigiGirls

IoT Attacks and Defense

- Case Study
- IoT and IoT Devices
- Smart Homes
- Smart Cities
- IoT Best Practices

An initiative of
cybersafe.
FOUNDATION

UKaid
from the British people

DigiGirls

Case Study

An initiative of
cybersafe.
FOUNDATION

Case Study

https://www.businesswire.com/news/home/20221129005177/en/Healthcare-Under-Cyberattack-Unprotected-Medical-IoT-Devices-Threaten-Patient-Care

Case Study

https://www.iottechnews.com/news/2022/dec/21/swatters-ring-cams-stream-victims-taunt-police/

An initiative of cybersafe. FOUNDATION

Case Study

https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

THANK YOU

UKaid
from the British people

DigiGirls

IoT and IoT Devices

An initiative of
cybersafe.
FOUNDATION

Internet of Things (IoT)

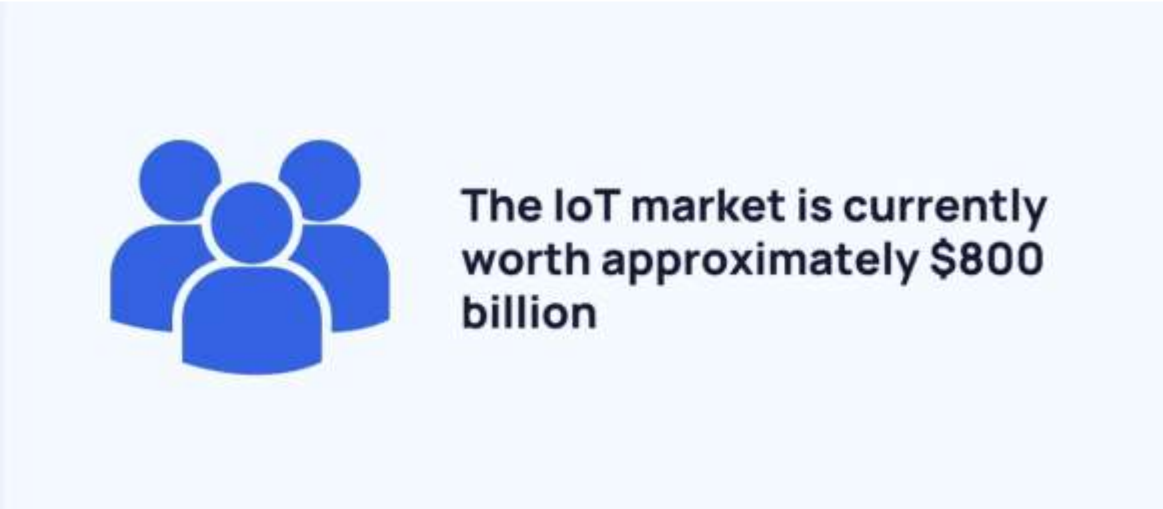
The internet of things, or IoT, is an interconnected network of computing devices, mechanical and digital machines, objects, animals, or people who are given unique identifiers (UIDs) and the capacity to transfer data over a network without the need for human-to-human or human-to-computer interaction.

Internet of Things (IoT)

The term "thing" refers to any natural or artificial object that can be given an Internet Protocol (IP) address and has the ability to transfer data over a network, including people with implanted heart monitors, farm animals with biochip transponders, cars with built-in tire pressure monitors, and other examples.

Internet of Things (IoT)

The number of IoT devices that are connected has increased significantly. and for the foreseeable future is predicted to increase year over year. There are approximately 13.15 billion connected IoT devices, based on the most recent data.

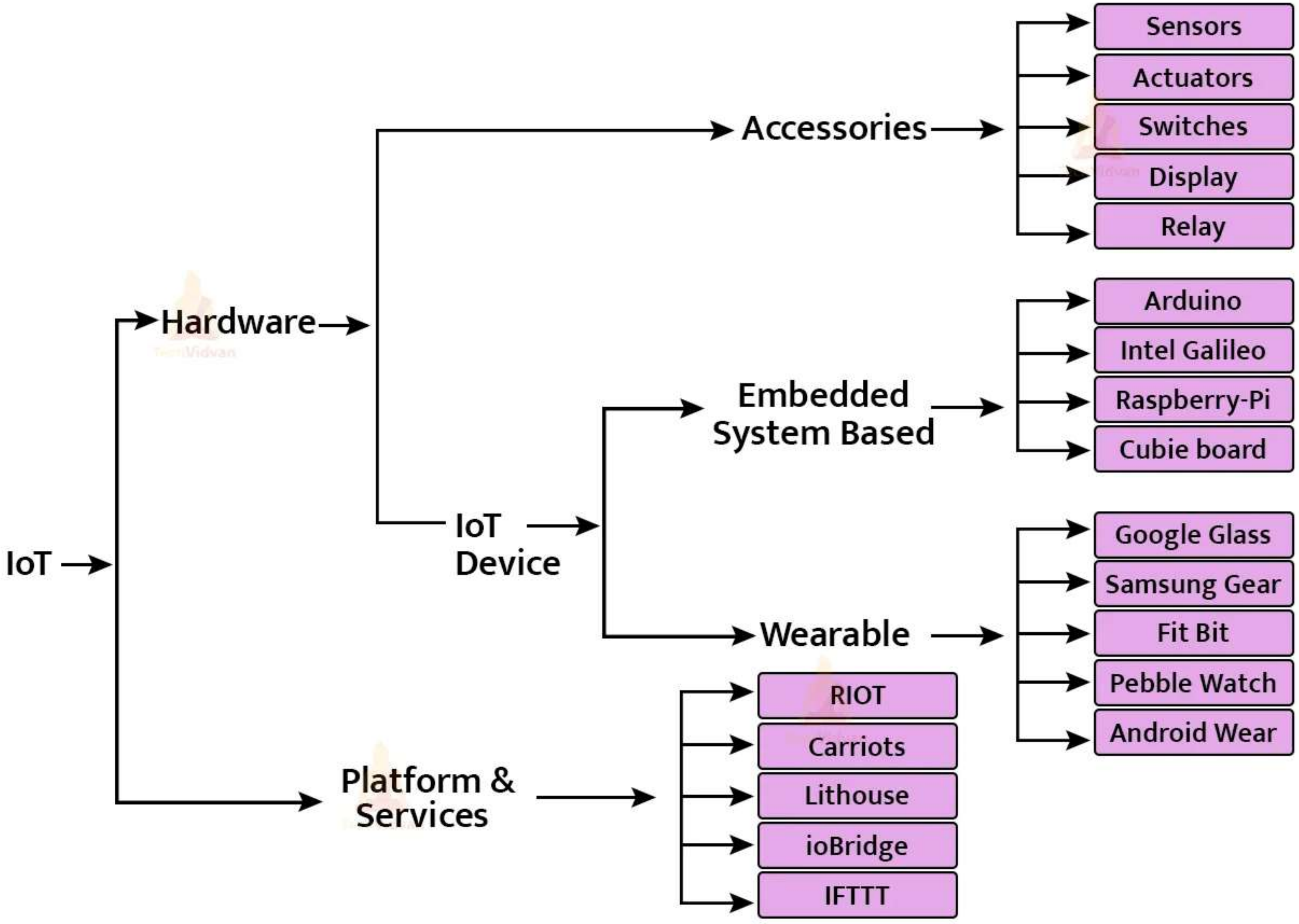


The IoT market is currently worth approximately $800 billion

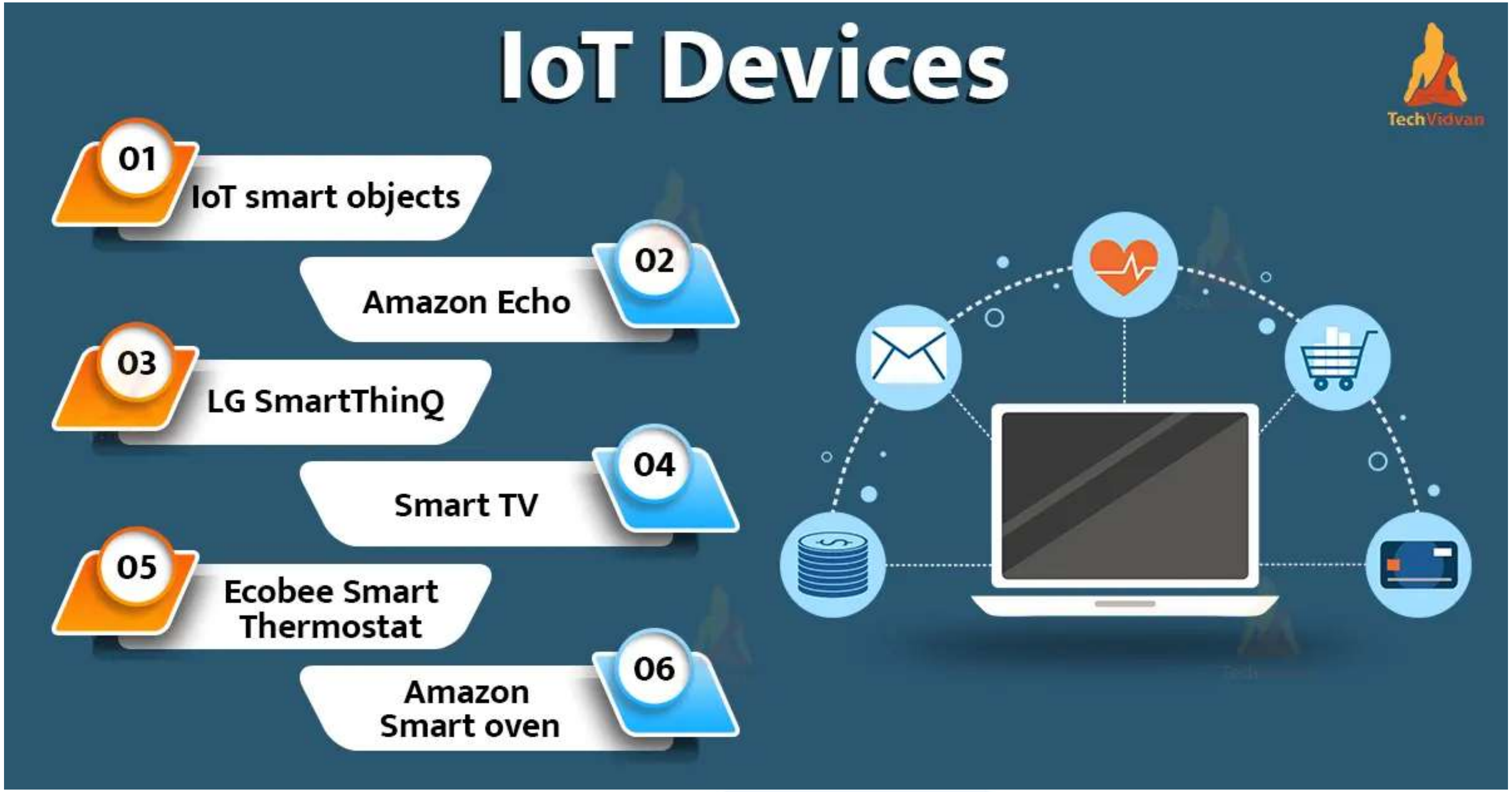
IoT Devices

Internet of Things devices are unconventional devices that are able to connect to a network and exchange data. The Internet of Things (IoT) expands connectivity to the Internet beyond conventional devices like smartphones, laptops, tablets, and desktops. Because these things are embedded with technology, we can communicate and interact with them across networks, and they can be remotely monitored and controlled.

IoT Devices and Technologies



An initiative of cybersafe. FOUNDATION



IoT Devices

01 IoT smart objects

02 Amazon Echo

03 LG SmartThinQ

04 Smart TV

05 Ecobee Smart Thermostat

06 Amazon Smart oven

Properties of IoT Devices

- **Sense:** The devices that sense their surrounding environment in the form of temperature, movement, the appearance of things, etc.
- **Send and receive data:** IoT devices are able to send and receive data over the network connection.
- **Analyze:** The devices can analyse the data received from the other device over the internet networks.
- **Controlled:** IoT devices may control from some endpoint also. Otherwise, the IoT devices communicate with each other endlessly, leading to system failure.

THANK YOU

Smart Homes

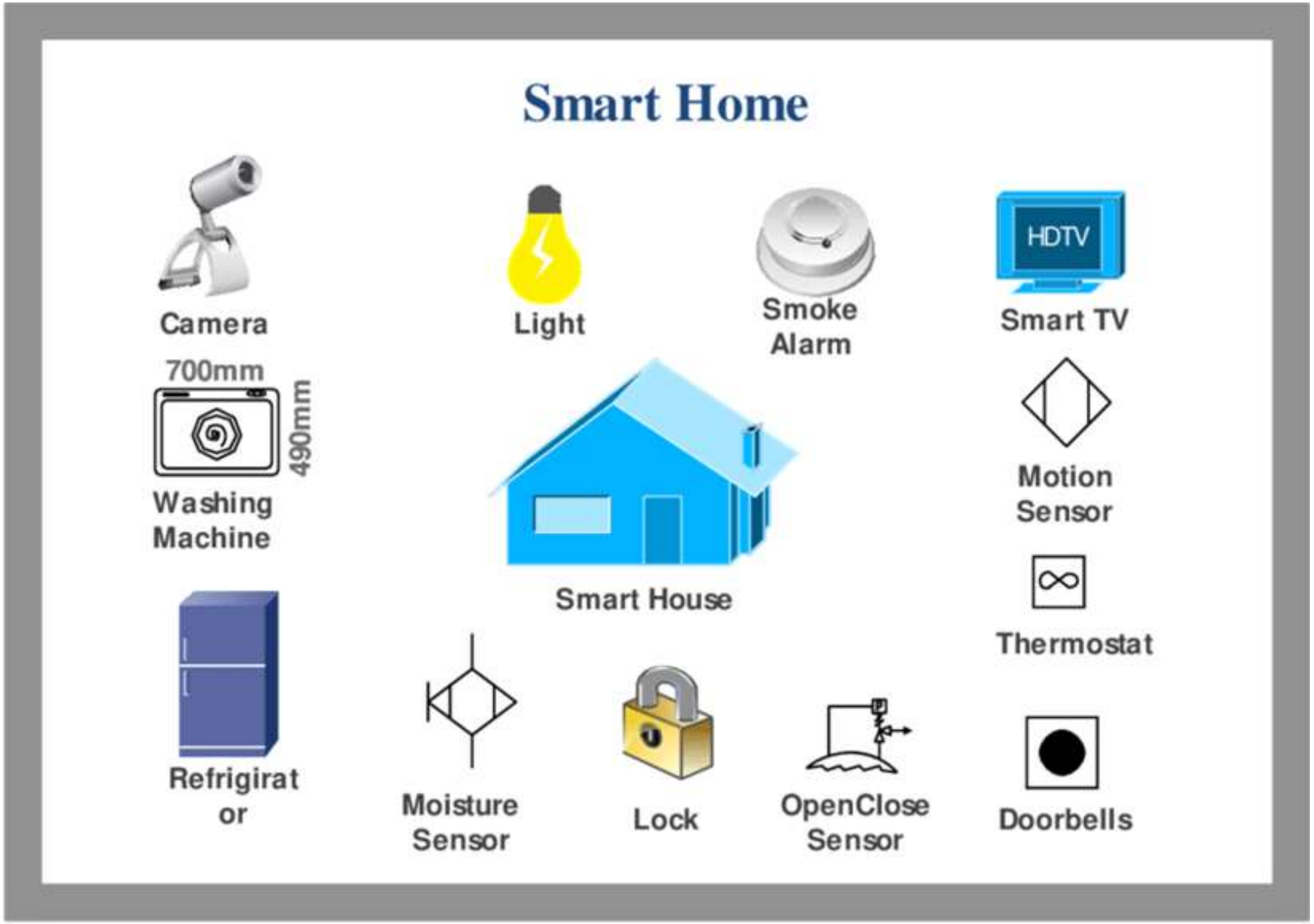
UKaid
from the British people

DigiGirls

An initiative of
cybersafe.
FOUNDATION

Smart Homes

A smart home is a convenient setup in which appliances and devices may be automatically controlled remotely using a mobile or networked device from anywhere with an internet connection. Devices in a smart home are interconnected via the internet, allowing the user to remotely control features such as home security, heating, lighting, and a home theatre.


Smart Home
Camera
Light
Smoke Alarm
HDTV
Smart TV
700mm
490mm
Washing Machine
Motion Sensor
Smart House
Thermostat
Refrigirat or
Moisture Sensor
Lock
OpenClose Sensor
Doorbells

Smart Home Device Attacks

Data Breach and Identity theft

Insecure IoT devices generate data and provide cyber attackers with ample space to target personal information. This could potentially end up in identity theft and fraudulent transactions.

Device hijacking and Spoofing

Smart devices can be hijacked, giving attackers complete control. The attackers can modify the device, spoof communication between two ends, and take control of other devices, or perhaps the entire network.

Smart Home Device Attacks

Distributed Denial of Service (DDoS)

The device or network resource goes unavailable to its intended users by temporarily or indefinitely disrupting the services.

Phlashing:

The device is ruthlessly damaged by such attacks to the point where it must be replaced.

Securing Smart Home Devices After Purchase

Use Strong passwords

Ensure routers and all devices have strong passwords. Hackers frequently use retained default passwords as entry points.

Guest Networks

When possible, use the guest network to connect smart home devices. This can assist in separating the devices from the sensitive data stored on laptops or phones. Even if cybercriminals infiltrate one of the IoT devices, they will not be able to breach the main network and compromise the PCs and smartphones that are connected to it.

Securing Smart Home Devices After Purchase

Two-factor authentication

Enabling two-factor authentication, which needs additional verification via a mobile or authenticator app, significantly decreases hackers' ability to modify devices.

Highest Level Encryption

Use the highest-level encryption (WPA3) on the router to ensure secure communication.

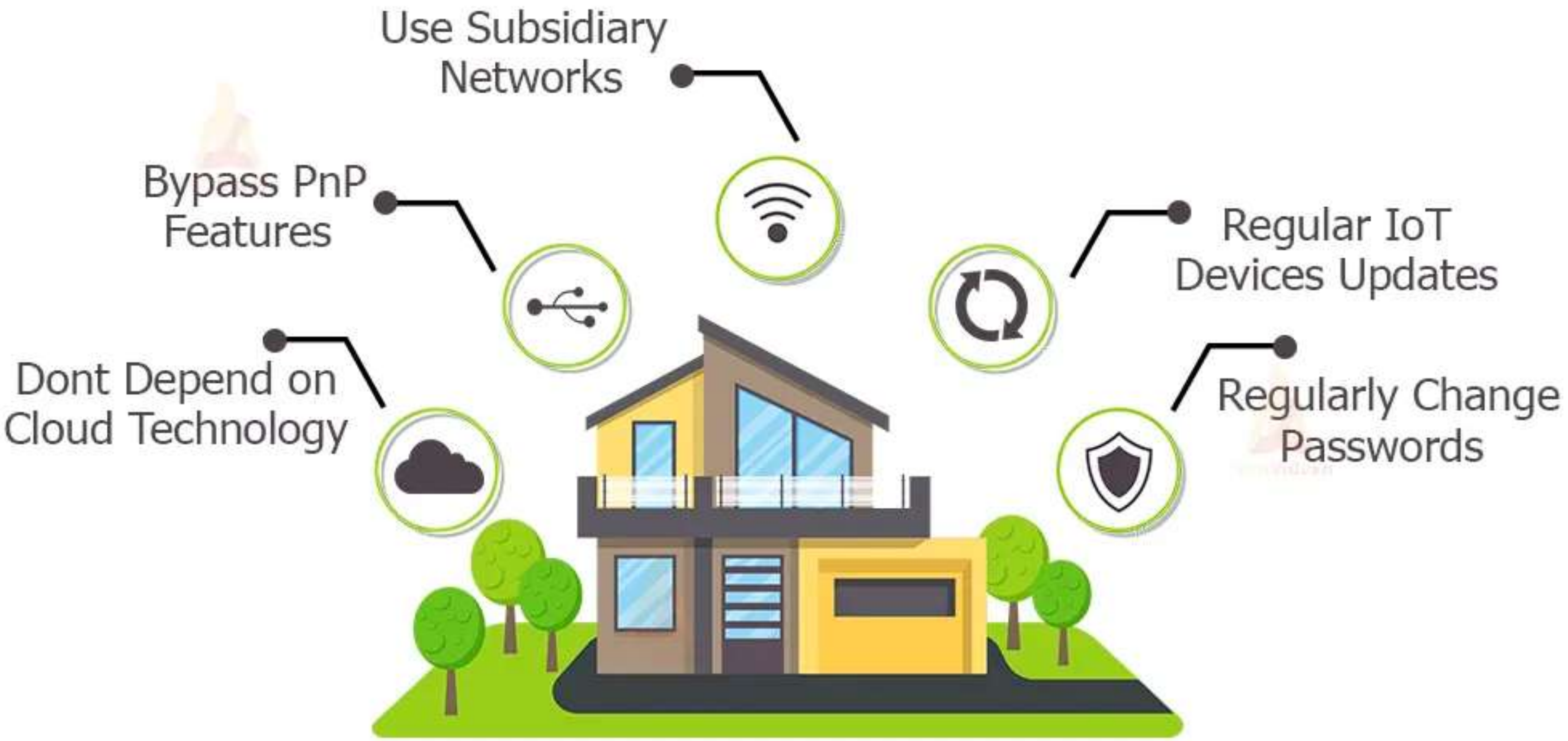
Securing Smart Home Devices After Purchase

Firewalls

Using firewalls is one of the famous ways to secure smart home devices. A firewall enables the user to see potential attacks and manage the security level of individual connected devices. Firewalls send notifications to the host when any abnormality in the network or devices is detected.

You can leverage the built-in firewall feature of your home router or get a dedicated firewall for your smart home.

Smart Home Security


Use Subsidiary Networks
Bypass PnP Features
Regular IoT Devices Updates
Dont Depend on Cloud Technology
Regularly Change Passwords

An initiative of cybersafe. FOUNDATION

UKaid
from the British people

DigiGirls

THANK YOU

An initiative of
cybersafe.
FOUNDATION

UKaid
from the British people

DigiGirls

Smart Cities

An initiative of
cybersafe.
FOUNDATION

IoT and the Smart City

Smart cities use IoT devices such as connected sensors, lights, and meters to collect and analyze data. The cities then use this data to improve infrastructure, public utilities and services, and more.

IoT forms the technical backbone of every smart city in the world, equipping them with the intelligence, interconnection, and instruments needed to improve urban services, optimize resources, and reduce costs. By connecting various devices, systems, and people, IoT can provide real-time data and insights on city operations and infrastructure.

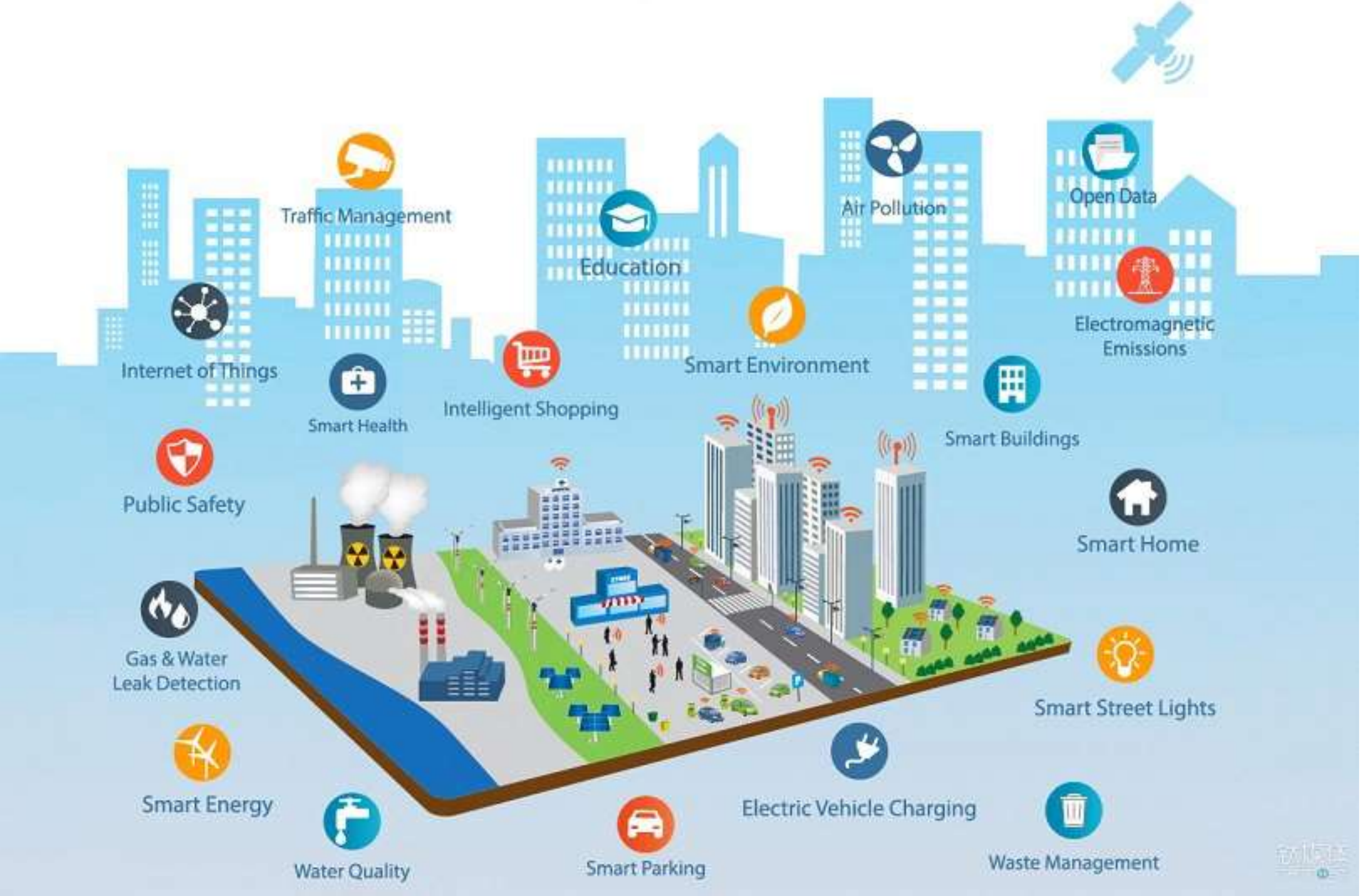
IoT and the Smart City

However, there are some distinct challenges in fully realizing the vision of a smart city – with security being the biggest concern at present. To this end, the interconnectedness of IoT devices creates new vulnerabilities for cyberattacks, data breaches, and unauthorized access.

Smart City Technologies

The foundation of smart cities relies on the utilization of Internet of Things (IoT) devices and networks. These devices, in combination with software solutions, user interfaces, and communication networks, enable and enhance the functioning and efficiency of smart cities.

An initiative of cybersafe. FOUNDATION


Traffic Management
Education
Air Pollution
Open Data
Internet of Things
Smart Environment
Electromagnetic Emissions
Smart Health
Intelligent Shopping
Smart Buildings
Public Safety
Smart Home
Gas & Water Leak Detection
Smart Street Lights
Smart Energy
Electric Vehicle Charging
Water Quality
Smart Parking
Waste Management

Smart Cities: Threat and Countermeasures

Around the world, smart cities have deployed billions of connected 'things'. The growth of the Internet of Things (IoT) presents a variety of vulnerabilities that cybercriminals and other bad actors can take advantage of. Smart cities are intended to boost productivity and efficiency, but if cyber security is not taken seriously, they could pose significant risks to both citizens and the government. There are untold numbers of methods and potential vulnerabilities.

Smart Cities: Threats

Data and identity theft

Data generated by unprotected smart city infrastructure such as parking garages, EV charging stations and surveillance feeds provide cyber attackers with an ample amount of targeted personal information that can potentially be exploited for fraudulent transactions and identify theft.

Man-in-the-middle

An attacker breaches, disrupts or spoofs communications between two systems. For example, a man-in-the-middle attack on a smart valve in a wastewater system may be exploited to produce a biohazard leak.

Smart Cities: Threats

Device hijacking

The attacker hijacks and effectively assumes control of a device. These attacks can be difficult to detect because in many cases, the attacker does not alter the basic functionality of the device. In the context of a smart city, a cyber-criminal could exploit hijacked smart meters to launch ransomware attacks on Energy Management Systems (EMS) or stealthily siphon energy from a municipality.

Permanent Denial of Service (PDoS):

Permanent denial- of-service attacks (PDoS), also known loosely as phlashing, is an attack that damages the device so badly that it requires replacement or reinstallation of hardware. In a smart city scenario, a hijacked parking meter could also fall victim to sabotage and would have to be replaced.

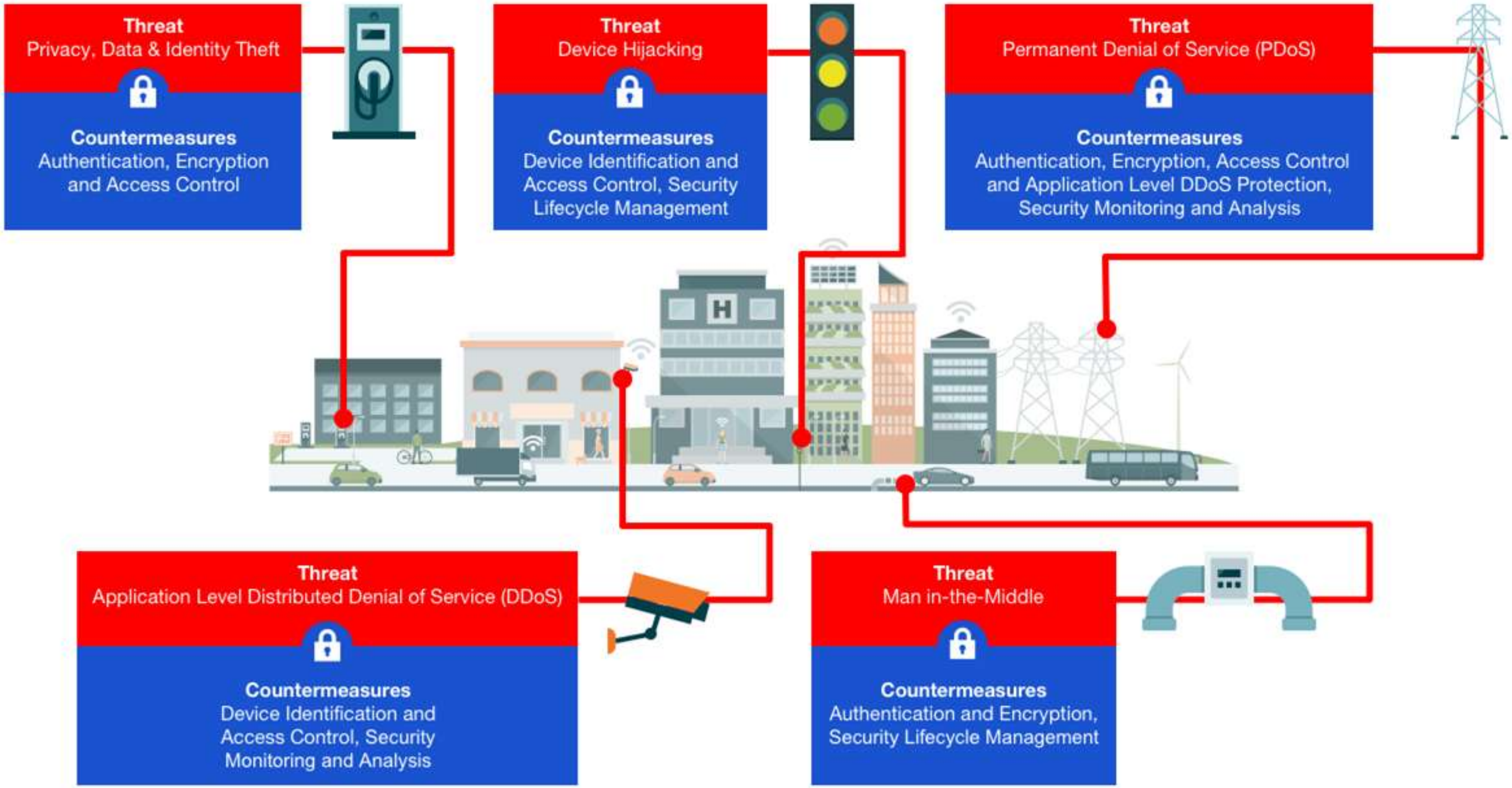
Smart Cities: Threats

Distributed Denial of Service (DDoS)

A denial-of-service (DoS) attack attempts to make a machine or network resource unavailable to its intended users by disrupting the services of a host connected to the Internet, either temporarily or permanently. This is usually accomplished by flooding the target with unnecessary requests in order to prevent legitimate requests from being fulfilled. In the case of a distributed denial-of-service (DDoS) attack, the incoming traffic flooding a target comes from multiple sources, making it difficult to stop the cyber offensive by blocking a single source. A variety of smart city equipment, such as parking meters, can be compromised and made to join a botnet programmed to overwhelm a system by requesting service at the same time.

UKaid
from the British people

DigiGirls



Threat
Privacy, Data & Identity Theft

Countermeasures
Authentication, Encryption and Access Control

Threat
Device Hijacking

Countermeasures
Device Identification and Access Control, Security Lifecycle Management

Threat
Permanent Denial of Service (PDoS)

Countermeasures
Authentication, Encryption, Access Control and Application Level DDoS Protection, Security Monitoring and Analysis

Threat
Application Level Distributed Denial of Service (DDoS)

Countermeasures
Device Identification and Access Control, Security Monitoring and Analysis

Threat
Man in-the-Middle

Countermeasures
Authentication and Encryption, Security Lifecycle Management

An initiative of
cybersafe.
FOUNDATION

UKaid
from the British people

DigiGirls

THANK YOU

An initiative of
cybersafe.
FOUNDATION

UKaid
from the British people

DigiGirls

IoT Best Practices

An initiative of
cybersafe.
FOUNDATION

UKaid
from the British people

DigiGirls

IoT Best Practices

1. Track and manage your devices.
2. Update your devices and apply patches regularly.
3. Update passwords and credentials.
4. Use up-to-date encryption protocols.
5. Conduct penetration testing or evaluation.
6. Understand your endpoints.
7. Segment your network.
8. Use multi-factor authentication.

An initiative of
cybersafe.
FOUNDATION

Topic Activity

https://www.businesswire.com/news/home/20221129005177/en/Healthcare-Under-Cyberattack-Unprotected-Medical-IoT-Devices-Threaten-Patient-Care

THANK YOU

UKaid
from the British people

DigiGirls

THE RISE OF INTELLIGENT MACHINES

An initiative of
cybersafe.
FOUNDATION

UKaid
from the British people

DigiGirls

Content

What is AI?

Risks Associated with AI

Protecting Yourself from AI Risks

Safe Use of AI Software

ChatGPT

An initiative of
cybersafe.
FOUNDATION

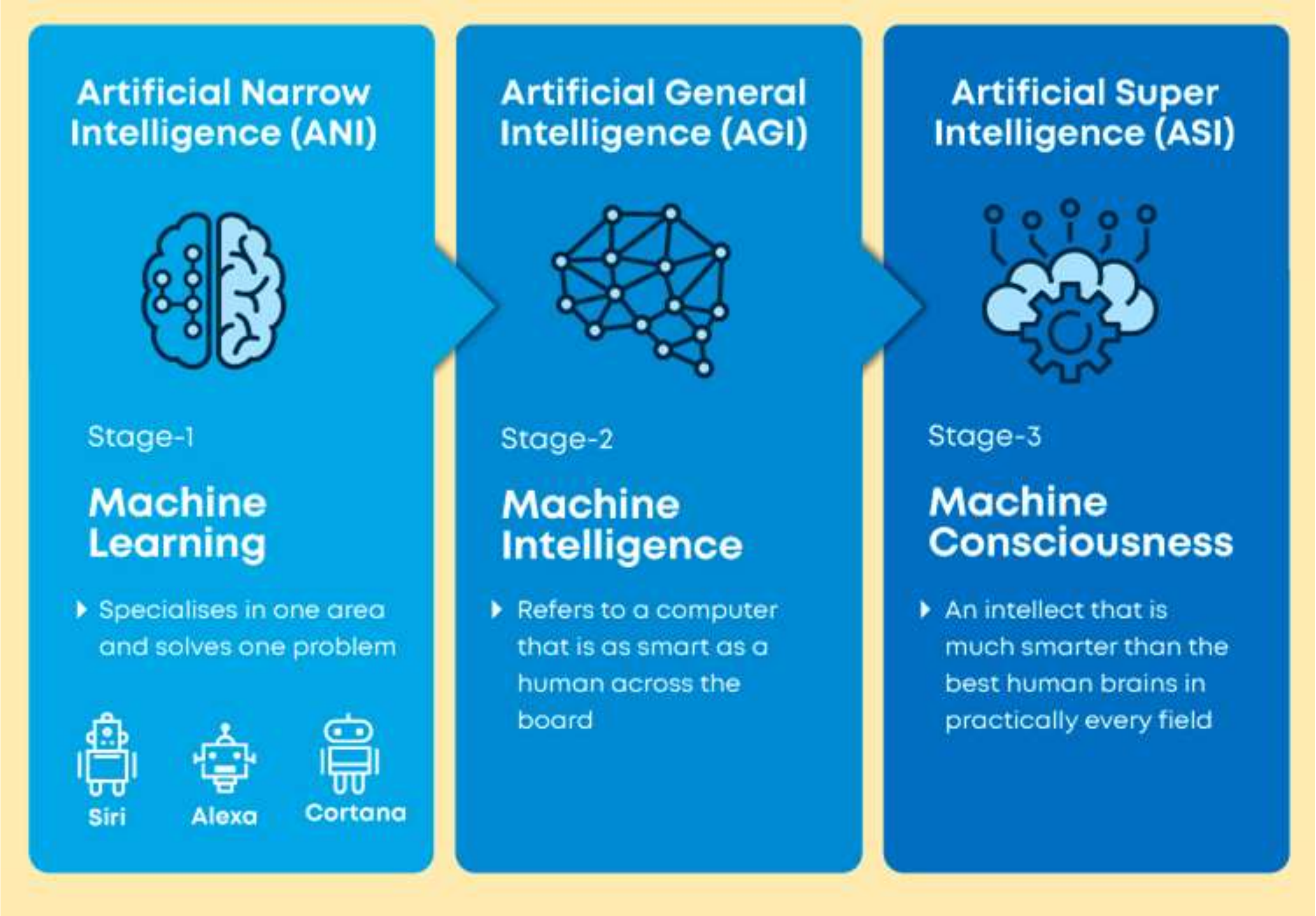
What is AI?

Artificial Intelligence

Machines can learn from experience, adapt to new inputs, and execute human-like jobs because of artificial intelligence (AI). Most AI examples you hear about today rely largely on deep learning and natural language processing, from chess-playing computers to self-driving cars.

AI uses data to automate repetitive learning and discoveries. AI performs regular, high-volume automated tasks rather than automating manual ones. And it does so consistently and without exhaustion. Of course, humans are still required to configure the system and ask the appropriate questions.

3 Types of Artificial Intelligence



Artificial Narrow Intelligence (ANI)

Stage-1

Machine Learning

- Specialises in one area and solves one problem

Artificial General Intelligence (AGI)

Stage-2

Machine Intelligence

- Refers to a computer that is as smart as a human across the board

Artificial Super Intelligence (ASI)

Stage-3

Machine Consciousness

- An intellect that is much smarter than the best human brains in practically every field

An initiative of cybersafe. FOUNDATION

Machine Learning

Machine learning is an artificial intelligence application that employs statistical approaches that enable computers to learn and make decisions without being explicitly programmed. It is based on the idea that computers can learn from data, recognize patterns, and make decisions with little help from humans.

It is a subset of AI. It is the study of how to make machines more human-like in their behaviour and decisions by allowing them to learn and generate their own programs. This is accomplished with as little human intervention as possible, i.e. no explicit programming. The learning process is automated and enhanced over time depending on the experiences of the machines.

Deep Learning

Deep learning is a branch of machine learning that trains a computer to perform tasks similar to humans, like speech recognition, image recognition, and prediction making. It strengthens the capacity to categorize, identify, detect, and characterize utilizing data. Deep learning is currently popular because of the buzz surrounding artificial intelligence (AI), in part.

Think of common systems like Siri and Cortana. Deep learning is used in part to power these.

THANK YOU

An initiative of cybersafe. FOUNDATION

UKaid
from the British people

DigiGirls

Risks Associated with AI

An initiative of
cybersafe.
FOUNDATION

Risks of AI

Technological risk—data confidentiality

The secrecy of data is the main technological risk. The advent of AI has made it possible to gather, store, and process information on a previously unimaginable scale, making it incredibly simple to identify, examine, and utilize personal data without others' consent. One of the main causes of customer anxiety and mistrust is the possibility of privacy leaks when using AI technologies.

Risks of AI

Technological risk—security

AI algorithms are the variables that optimize the training data, which gives the AI the capacity to provide insights. If an algorithm's parameters are revealed, a third party might be able to reproduce the model, costing the model's owner money and loss of intellectual property. Additionally, if an online hacker were to change the AI algorithm model's settings without authorization, the AI model's performance would suffer and unpleasant outcomes would follow.

Risks of AI

Usage risk—abuse

The possibility of misuse exists even when an AI system is doing its analysis, decision-making, coordination, and other tasks successfully. It is possible for the operator's use purpose, use technique, use range, and other elements to be corrupted or altered with the intention of causing negative impacts. One example is using face recognition to follow people's movements without their consent.

Risks of AI

Usage risk—inaccuracy

The data that an AI system learns from has a significant impact on how well it performs. Even if an AI system is technically sound, it will produce unfavorable results if it is trained on biased, erroneous, or stolen data.

UKaid
from the British people

DigiGirls

Topic Activity

In your peer learning groups, discuss the possibility of AI rising against the human race.

An initiative of
cybersafe.
FOUNDATION

THANK YOU

An initiative of cybersafe. FOUNDATION

UKaid
from the British people

DigiGirls

Protecting Yourself from AI Risks

An initiative of
cybersafe.
FOUNDATION

How to Protect Yourself from AI Risks

Limit Online Presence: Limit the amount of personal information, images, and voice recordings you share online. Be cautious about the type and amount of data you share on social media, websites, or other online platforms, as this data could be used by AI systems for various purposes.

Use Privacy Settings: Utilize privacy settings on social media and other online platforms to control who can access and use your images and voice recordings. Review and adjust your privacy settings to ensure that your personal data is only visible to the intended audience.

How to Protect Yourself from AI Risks

Read Terms of Service: When using online platforms that involve uploading images or voice recordings, carefully review the terms of service and privacy policies. Understand how your data may be used by the platform and whether they have any rights or permissions to use your content. Understand the consequences of using those social media apps where you put in information and your photo to get a nickname and avatar image – there is almost always a data usage acceptance behind the scenes that you don’t know about unless you look carefully

How to Protect Yourself from AI Risks

Be Cautious with Voice Recordings: Be careful while sharing your voice recordings, especially with unproven or new AI services or applications. Be careful of the possible dangers of voice cloning or voice manipulation and refrain from providing private or sensitive information over voice recordings.

Monitor for Misuse: Regularly monitor the internet for any unauthorized use of your images or voice recordings. You can use reverse image search tools or other monitoring techniques to identify any instances of AI-generated content that may be misusing your image or voice.

THANK YOU

UKaid
from the British people

DigiGirls

Safe Use of AI Software

An initiative of
cybersafe.
FOUNDATION

UKaid
from the British people

DigiGirls

Common AI Software

- ChatGPT
- Jupyter Notebooks
- Google Cloud AI Platform
- Azure Machine Learning Studio
- Infosys Nia
- Salesforce Einstein
- Chorus.ai
- Observe.AI Software
- DataRobot
- Tractable
- Content DNA Platform

An initiative of
cybersafe.
FOUNDATION

Safe Use of AI Software

- Understand that AI-powered technologies are by no means secure by design.
- Using AI software to generate content is an effective way to produce ideas or overcome small writer's block. However, depending on the text to provide you with the information is risky. Every fact must be double-checked, and the same applies to software code or ChatGPT answers.
- Be mindful of the information you share with AI Software e.g. information that reveal sensitive data such as PII, images, payment card details etc.

Safe Use of AI Software

- Be mindful of the kind of permission you give to AI software applications on your PCs and smartphones
- Protect all data using various protective technologies on different platforms
- Stop, Think, Share

Topic Activity

Examine the Stupidity of AI

https://www.theguardian.com/technology/2023/mar/16/the-stupidity-of-ai-artificial-intelligence-dall-e-chatgpt

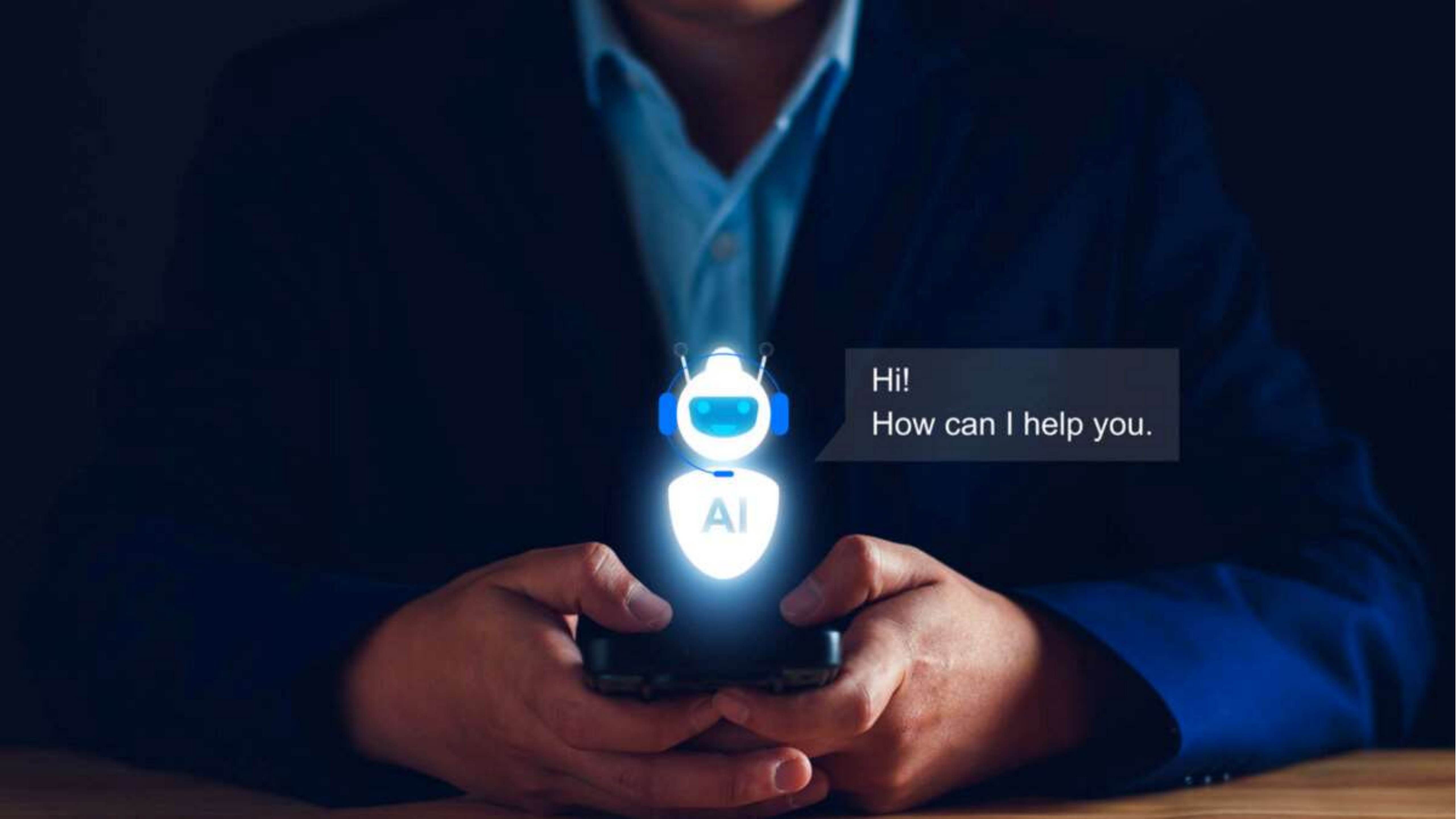
UKaid
from the British people

DigiGirls

THANK YOU

An initiative of
cybersafe.
FOUNDATION

ChatGPT


Hi!
How can I help you.
AI

Case Study

ChatGPT Data Breach

https://securityintelligence.com/articles/chatgpt-confirms-data-breach/

An initiative of cybersafe. FOUNDATION

ChatGPT

OpenAI created ChatGPT, an AI chatbot made public in November 2022. The name "ChatGPT" combines the words "Chat," which refers to the chatbot feature, and "GPT," which is short for generative pre-trained transformer and refers to a particular kind of big language model.

ChatGPT stands apart from other chatbots because of its reinforcement learning from human feedback model, which allows it to produce natural language, to understand when it has made mistakes, and more.

Risks Associated with ChatGPT

Data privacy and confidentiality: Any information entered into ChatGPT, if chat history is not disabled, may become a part of its training dataset. Sensitive, proprietary or confidential information used in prompts may be incorporated into responses for other users

Intellectual property (IP) and copyright risks: A significant amount of internet data, including maybe copyrighted material, was used to train ChatGPT in particular. Therefore, it's outputs could potentially breach copyright or intellectual property restrictions. ChatGPT does not include source citations or descriptions of how its output is produced.

Risks Associated with ChatGPT

Fabricated and inaccurate answers: The primary issue that users encounter with ChatGPT is a tendency to give inaccurate information that appears plausible at first glance.

Cyber fraud risks: False information is already being produced at scale by bad actors using ChatGPT, for example, fake reviews.

Consumer protection risks: Businesses who use ChatGPT without disclosing it to customers (for example, by using a chatbot for customer service) face the risk of losing those customers' trust and being accused of unfair business practices by a number of different legal authorities.

UKaid
from the British people

DigiGirls

ChatGPT Security Best Practices

- Never input personal identification information (PII)
- Turn off the toggle for “Chat History & Training”: Unchecking this option prevents ChatGPT from saving news talks to your history or using them to train models. Conversations that were not saved will be removed from the system within one month.
- Always verify the data you get from an AI tool before using it.
- Stay vigilant against phishing attacks.

An initiative of
cybersafe.
FOUNDATION

UKaid
from the British people

DigiGirls

ChatGPT Security Best Practices

- Before using a ChatGPT-powered app or any service that uses OpenAI language models, carefully review the platform's privacy policy and data handling policies to learn how the platform stores and uses your chats.
- Use anonymous or pseudonymous accounts. As a result, there will be less chance that your true identity will be linked to chat data.
- To ensure a high level of security while using ChatGPT, be informed of any changes to OpenAI's security measures or privacy policies and adjust how you operate accordingly.

An initiative of
cybersafe.
FOUNDATION

UKaid
from the British people

DigiGirls

THANK YOU

An initiative of
cybersafe.
FOUNDATION