

e-Devices

What digital devices features and applications do I use and what do others use to make life easier

e-Devices

- I encourage you in this session to share what you like and dislike about the e-Devices you use
- I will prompt and cajole you to provide your favorite application/s
- I will ask you to talk about your least useful applications (why?) as your experience may be based on hard earned frustration.

e-Devices

- As a back-up I have prepared some slides which describe some aspects of the IT world which are of social and business relevance
- Phishing
- Blockchain Technology
- .

E-Devcies

- Some of the applications discussed this year and last year that were thought to be useful
 - Rome2Rio
 - XEcurrency converter
 - XpenseTracker
 - Uber
 - Bookings.com
 - Airbnb
 - FlightTracker
 - Owl Intuition
 - MagicPlan
 - Wordflex
 - WPS
 - Whatsapp/Wechat

e-Devices

- Phishing

Is the practice of sending emails purporting to be from reputable companies or trusted sources (work mates, clients, etc.) in order to induce or cause an individual to reveal personal information, such as passwords and credit card numbers without that individual's knowledge

- Why should you be concerned?
- What does it look like?
 - Email
 - Friend Request

e-Devices

- Message from your ISP asking you to login to check some detail
- Account expiration
- Alert that your email password has been used by someone
- False shopping site
- Virus threat
- Scanned an error on your computer

e-Devices

Subject: Suspension



Dear Client, ← Generic non-personalized greeting

We have sent you this e-mail, because we have strong reason to believe, your account has been used by someone else. In order to prevent any fraudulent activity from occurring we are required to open an investigation into this matter. We've locked your Amazon account, and you have 36 hours to verify it, or we have the right to terminate it.

To confirm your identity with us click the link below:

<https://www.amazon.com/exec/obidos/sign-in.html>

← Hovering over the link reveals it points to a non-Amazon site - "http://redirect.kereskedj.com"

Sincerely,
The Amazon Associates Team



e-Devices

From: American Express <services@americanexpress.c...> Sent: Wed 9/21/2011 11:59 AM
To: undisclosed-recipients
Cc:
Subject: To Restore Your Account Acces You must verfiy Your Information



Dear American Express Client,

Phishing

This is an automatic message by the system to let you know that you have to confirm your account information within 24 hours.

Your account has been frozen temporarily in order to protect it. The account will continue to be frozen until it is approved. Once you have updated your account records, your information will be confirmed and your account will start to work as normal once again.

This will help protect you in the future. The process does not take more than 5 minutes.

To proceed to confirm your account information please click on the link below and follow the instructions that will be required.

[Click Here To Verfiy Your Account info](#)

e-Devices

- Increasingly sophisticated
 - Targeting the employees of your firm
 - By learning about them from their social media account
 - Sending them a link or a request from one of their friends including information that would lead them to think that the message is from that friend
 - What is in the link may not have an immediate consequence
 - The link could insert code to:
 - Record and transmit back to base keystrokes (includes passwords and other information)
 - Copy and transmit documents
 - Contain ransom ware

e-Devices

- What is ransom ware?
 - a type of software designed to block access to a computer system until a sum of money is paid.
- How does it work?
 - The software that is downloaded uses a key specific to the downloading computer (which the software obtains from a file located external to the downloading computer or the network that computer is on- typically and in the cloud) and uses that key to encrypt some or all of the files on that computer.
 - The software may also be transported throughout the network and do the same as above to one or more of the computers in the network, including servers in that network.

e-Devices

- There are two parts to the key one which can be seen on the computer but the other part is secret and kept in the cloud (command and control servers) and the way they work together means that only the key in the cloud can be used to unlock the files that have been encrypted with the key on the computer
- Until recently the way to defeat this arrangement was to detect the code that infects the downloading computer and then isolate the code from obtaining the key stored in the cloud by restricting access of the computer to the internet

e-Devices

- The creators of that arrangement have now worked out how to avoid that defense
 - They now use a key which is sent with the downloaded code that will immediately begin to encrypt the files
 - This is not an ideal way to do this but will still adversely affect those that do not know what to do
 - The solution to this arrangement is to know the unlocking key which will be the same for all the infections and that can and will be determined over time
- Take note that the purveyors of this arrangement use massive attack volumes e.g. 120,000 attack per hour

eDevices

- BLOCKCHAIN
- Is a distributed database that is open to everyone to access but which since it is distributed means that when someone changes an entry that entry is made to every copy of that database
 - Think of it as a public ledger
 - What is recorded in that ledger is up to the developer
 - The first and most famous use is the creation of a digital representation of a unit of value called a bitcoin.

eDevices

- What is a bitcoin?
 - A type of digital currency
 - It is not the ONLY form of cryptocurrency examples of alternatives include:
 - Litecoin –advantage processed more quickly
 - Peercoin –advantage more environmentally sustainable
 - Primecoin – based on sequences of prime numbers
 - Namecoin- based on dot.bit domains
 - Ripple – the advantage could be that it is backed by Google
 - Quark- uses 9 rounds of encryption to secure its owners
 - Freicoin –difference is that the value for those that do not use the currency devalues by 5% each year of non-use
 - And 13 more

eDevices

- How is a bitcoin it created?
- Each new coin is generated by solving a highly mathematical



Problem on very specialised computers (at least they are now since the early miners (the term used to describe people that perform this task) were tasked with solving that problem when the first solutions were plentiful

- However, now the computing power (indeed the electrical power consumption per cycle is a factor 0 is now much greater that previously the case

eDevcies

- What happens to my bitcoin that has been created?
 - The bitcoin software that everyone that has a bitcoin does a number of things
 - It maintains a block which is the unique sum of the digital data that represents a bitcoin
 - To do that it uses a mathematical algorithm to uniquely identify that particular block at a particular time called a HASH
 - A HASH algorithm is mathematically proven to have a property which can accept a string of data and create a unique representation of that string but knowing the string does not allow you to work out what that string was/is
 - Most importantly if the original string of data is changed in ANYWAY the same HASH will create a different representation

eDevices

- It is that property of the HASH that makes it possible to be sure that your bitcoin is exactly the same bitcoin forever, because your identity is included in another HASH of that same bitcoin and the combined data string creates another unique identity which becomes part of the block –referred to as a blockchain
- When you then distribute these created blockchains to everyone that has a bitcoin or bitcoin register and thus a register of all the bitcoins ever generated is thus available to everyone
- Now there is surety that the bitcoin and its especially its owner cannot be changed without everyone in the network noting that the fraudulent bitcoin or owner does not match the earlier record
- When ownership changes (with the permission of the owner) the blockchain changes include the identity of the new owner and all the previous changes are preserved in the blockchain

eDevice

- Now that you understand the basics of blockchains using the cryptocurrency model how else can you apply this technology?
 - one implementation of blockchains allows users to write sophisticated smart contracts, and creating invoices that pay themselves when a shipment arrives or share certificates which automatically send their owners dividends if profits reach a certain level.
 - regulatory bodies in the music industry have started testing models that use blockchain technology for royalty collection and management of copyrights around the world

e-Devices

- What should be apparent is that blockchain technology is a different for of ledger
 - Could they be used for recording the signature of a diamond –yes already that is the case
 - Could they be used instead of a patent ownership ledger –not yet buy why not
 - Could they be an alternative to a land title – why not,
 - Scientific publications records
 - Claims to copyright of a digital file
 - Payment confirmation systems; ,
 - Learning, employment, credit history
 - Voting
 - Email veracity mechanism
 - Veracity of public information about government and corporates

Note there would be no centralised record it would exist on hundreds if not thousands of computers

E-Devices

I will provide a list to all attendees of the various applications that were provided by you today on the sheet that circulated during the session so that you can review whether they are suited to your needs.