



# **CYBER JAGROOKTA DIWAS WEEK 2**

## **CYBER SECURITY AWARENESS**

Advice for Individuals and  
Businesses



# The Risks Behind the Apps

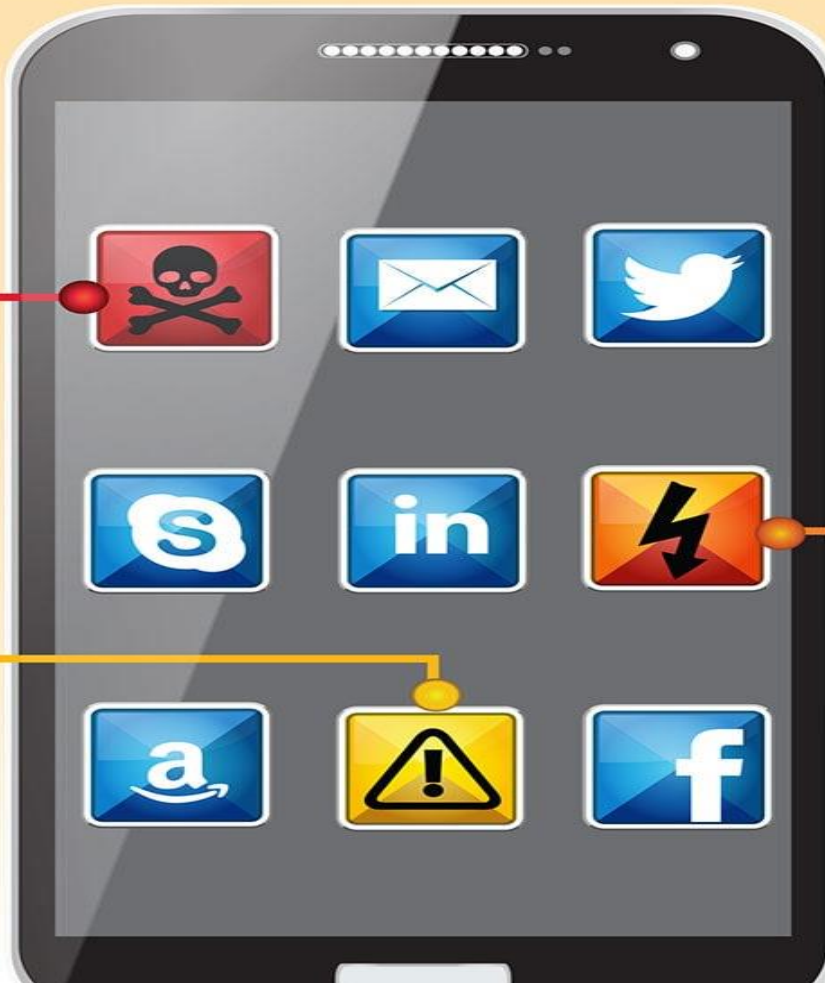
## Malicious Behaviors

- Accesses device management and restricted security APIs unnecessarily
- Accesses or requests Super User permissions
- Exploits operating system or zero-day vulnerabilities
- Roots or jailbreaks device
- Steals login credentials
- Communicates with known malicious IP addresses and domains

## Moderate Risk Behaviors

*May be a risk if performed by apps from unknown or untrusted sources*

- Reads and Sends emails
- Reads and Sends SMS messages
- Reads and sends



## Dangerous Behaviors

- Uploads user information without permission or without notifying user
  - Upload address book without notifying user
  - Reads SMS messages and sends them off the device
  - Reads emails and sends them off the device
  - Reads browser history and sends it off the device
- Includes SSL vulnerabilities that enable communications to be intercepted
- No privacy policy or refers to an invalid privacy policy
- Installs boot-time startup item

# MOBILE DEVICES



## WHAT!?

Mobile devices are becoming a much bigger target for Cybercriminals.



## HOW?

Cybercriminals will use software hidden within links to hack a mobile device. They also use Apps that contain viruses. As well as this, connecting to an unsafe WIFI on your mobile device can also exploit sensitive data.



## WHY?

Our mobiles know everything about us these days as we store lots of sensitive data on there. It is an easy way for cyber criminals to find a way into a company. Users are often ignorant about the dangers...

## TOP TIPS:



1 Keep your mobile device and apps updated.



2 Be wise when using free WIFI and connecting to Bluetooth.



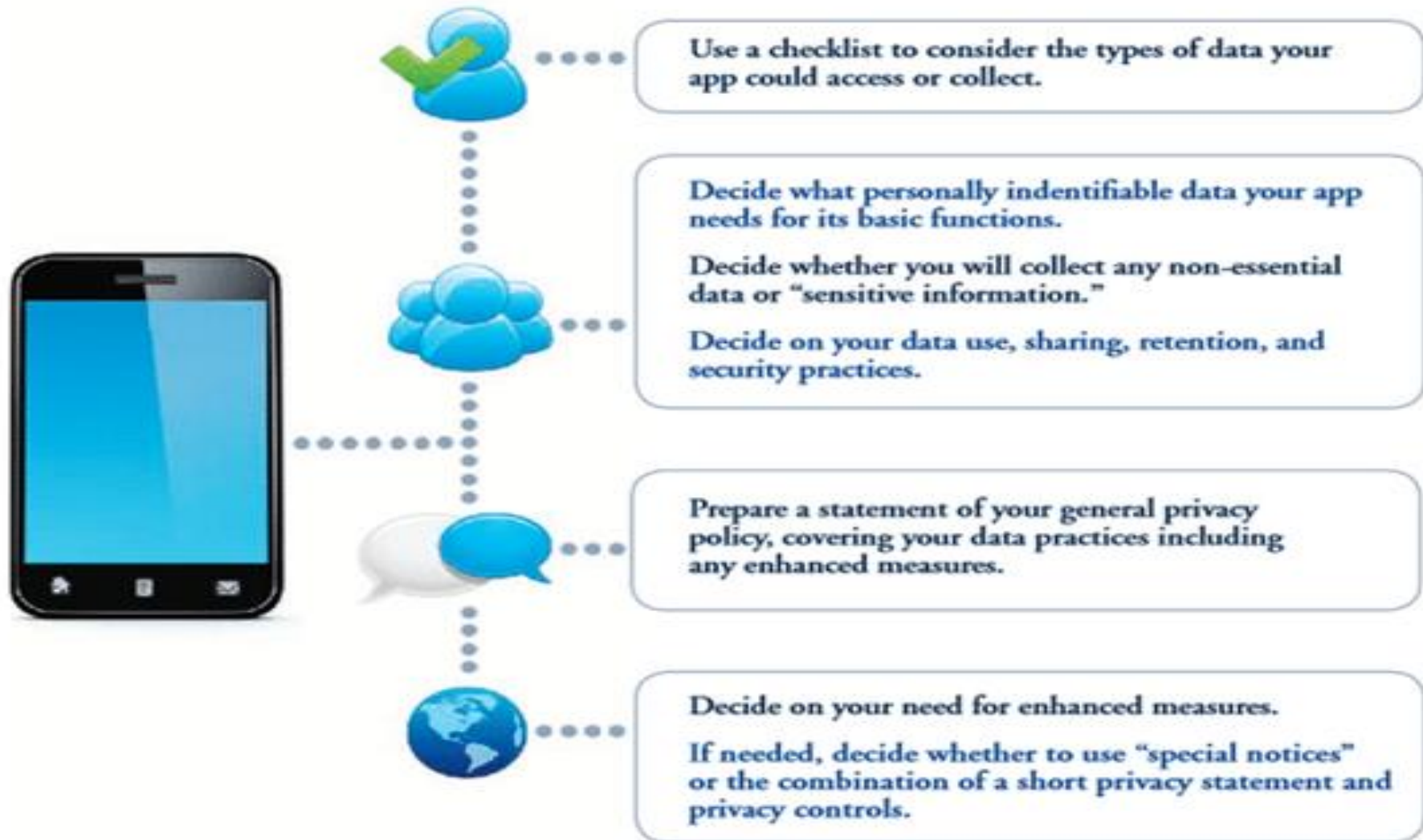
3 Use two-factor authentication whenever possible.



4 Be sure to back up your data, so if you are ever hacked you still have sensitive data stored.



## Decision Path for Building Privacy into Apps



# PRESENTATION CONTENTS

## Need for Cyber Security

### Threats:

- Hacking
- Malware
- Phishing

### Stay Secure

- Internet Shopping
- Internet Banking

## Personal Privacy

- Public Wi-Fi
- Passwords
- Router
- Internet of Things (IOT)

## QR Codes

## Support & Resources

# WHY IS CYBER AWARENESS IMPORTANT?

- Cyber crime is a growing trend.
- Raise awareness of threats As with most crimes the police can't tackle this problem alone.
- To encourage reporting Promote Government backed scheme.
- Cyber crime is massively under reported.

# HOW CYBER CRIME AFFECTS

Approximately 30% of the INDIA economy is online.

It poses a risk if the correct security measures aren't taken.

According to an Office for National Statistics Survey, there were almost 6 million Cyber Crime and Fraud offences in 2016 at UK, which means these crime types now make up half of all crime in England and Wales.

That's 1/10 of people in England and Wales.



**WHO IS DOING THE HACKING?**

# HACKING

Financial (theft, fraud, blackmail)

Political /state (state level/ military)

Fame/ kudos (fun/ status)

Hacktivism (cause)

Pen testers (legal hacking)

Police

Insider

Business

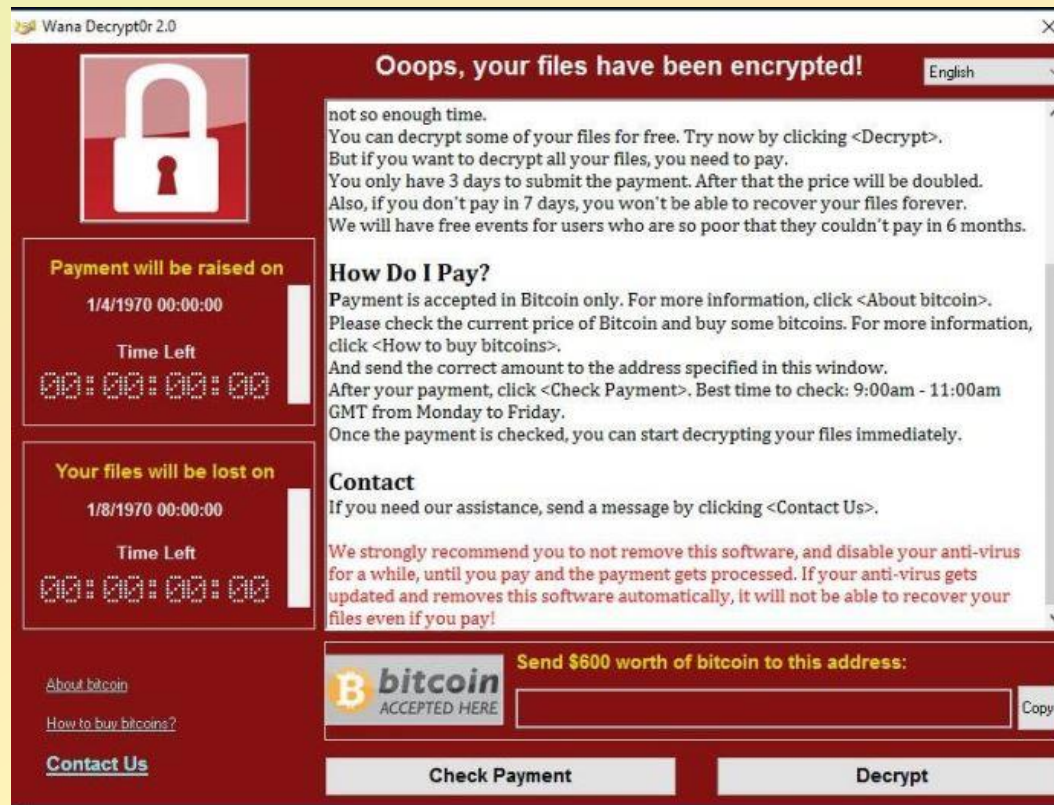


# COMMON THREATS - RANSOMWARE

- Normally loaded onto a computer via a download/attachment/link from an email or website.
- Will either lock the screen or encrypt your data.
- Once Ransomware is uploaded on your computer/tablet/phone it is very difficult to remove without removing all of the data
- Wannacry attack 2017 - One of the biggest cyber attacks to occur.
- Is said to have hit 300,000 computers in 150 countries.
- Companies affected include; NHS, Renault, FedEx, Spanish telecoms and gas companies, German railways.

# RANSOMWARE

- Message appearing like



# HOW TO TACKLE RANSOMWARE

- Back up- Keep a backed up copy of your data. Ensure its not permanently connected to the network.
- Patch- Keep your software up to date. Wannacry was successful as those affected computers hadn't updated. The update contained a fix for the problem.
- Attachments- Don't click on links from emails/SMS as this could easily be from an untrusted source and contain malware like Ransomware

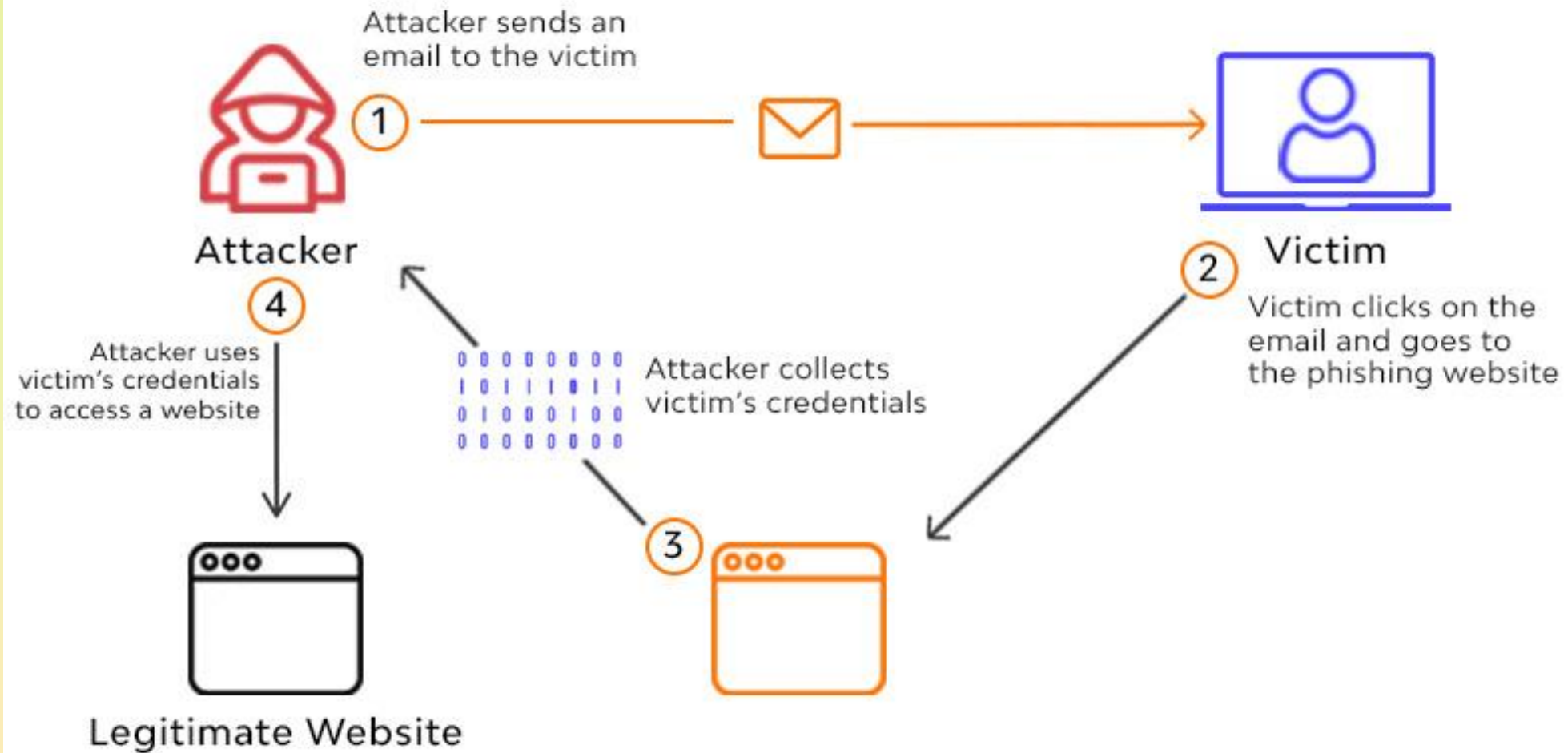
# PHISHING

- Is the attempt to obtain sensitive information by deception.
- They will be after your login credentials, payment card details or to upload malware to your computer
- The email will normally impersonate a genuine company or person.

## How to tackle the problem

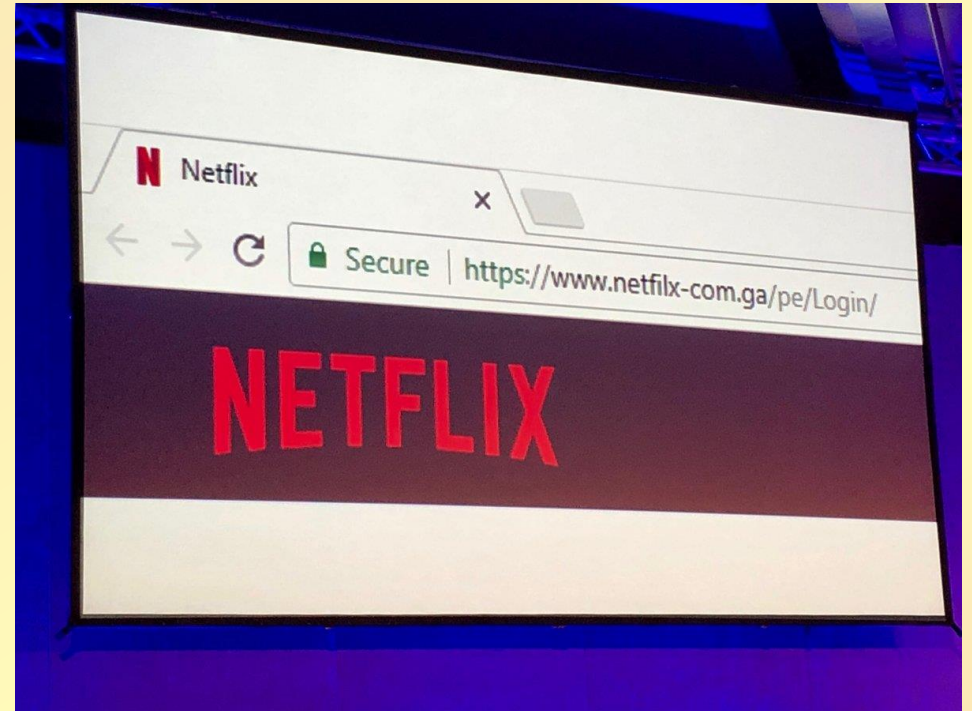
- Don't click any links on an email unless you can guarantee who its from.
- Use a trusted method of contacting the company via a phone number, app or website.
- Mark the email as spam and contact the organisation.





# WHAT TO LOOK OUT FOR WHEN SHOPPING ON THE INTERNET?

- Ensure you're on the correct website
- HTTPS and the padlock- The 'S' stands for secure, this means you have a secure connection to the website. This should prevent a 'man in the middle' attack. It encrypts your data and the receiver will be able to decrypt it but if it is a fraudulent website they will still obtain your information.
- Use a credit card/ UPI when conducting online transactions.





From: **NtWest** >

Hide

N

## New online login authentication procedures #NTWS-2563368

Today at 11:14



### Security Update

Please note that starting from March 13, 2017 we will be introducing new online banking authentication procedures in order to protect the information of our online banking users.

#### This is the security information that will be added to your account.

- Two-factor authentication
- Security Question

You are required to confirm your personal details with us as you will not be able access our online service until this has been done. As you're already registered for online banking all you need to do is to confirm your online banking details.

<https://natwest.co.uk/UpdateSecurity?Token=82NM119923020LWP>

Once you've completed this process you will be able to have full access to our online banking service.

Your new updated security information will be added to your account within 2 weeks of your account being verified.

#### It takes 2 minutes to protect yourself online

Anti-virus software alone isn't enough. Download our free IBM Trusteer Rapport security software, which:

- Confirms that you're connected to our website
- Shields your online banking details from prying eyes
- Protects your card details when shopping online

Download Rapport

### Security Update

Please note that starting from March 13, 2017 we will be introducing new online banking authentication procedures in order to protect the information of our online banking users.

#### This is the security information that will be added to your account.

- Two-factor authentication
- Security Question

You are required to confirm your personal details with us as you will not be able access our online service until this has been done. As you're already registered for online banking all you need to do is to confirm your online banking details.

<https://natwest.co.uk/UpdateSecurity?Token=82NM119923020LWP>

Once you've completed this process you will be able to have full access to our online banking service. Your new updated security information will be added to your account within 2 weeks of your account being verified.

#### It takes 2 minutes to protect yourself online

Anti-virus software alone isn't enough. Download our free IBM Trusteer Rapport security software, which:

- Confirms that you're connected to our website
- Shields your online banking details from prying eyes
- Protects your card details when shopping online


It's a simple two step process that only takes a few minutes, download then install the software

IBM Rapport works on PCs, laptops and Macs only. It is not available for Tablets / Mobile devices.



Mail 11:32 75%

www4-naatwet.com

 **NatWest** [Cookie policy](#)

Welcome

Customer number

Remember me. We don't recommend storing data on a shared computer.

[Continue](#)


[Forgotten any of your log in details?](#)

[Register for Internet Banking](#) >


[Go to desktop site](#) >


giffgaff 11:23 76%


Done




**NtWest**

 other

 call

 video

 other

other

[I.9799@caqwetiolo.com](mailto:I.9799@caqwetiolo.com)

[Add to VIP](#)



HSBC



Text Message  
Today 04:15

Our security team have tried to contact you regarding your online account. Log In via the secure link <http://209.177.93.144> to reactivate.



Lloyds



Text Message  
Today 14:59

We have tried to contact you about your Internet Banking account, we have limited your account due to recent activity. Visit the secure <http://199.245.58.9> link



Halifax

[redacted] from abroad

Sat 2 Dec, 16:05

Your new statement for credit card ending [redacted] is ready to view, please sign in to Online Banking for further details.

Fri 15 Dec, 12:06

Your new statement for credit card ending [redacted] is ready to view, please sign in to Online Banking for further details.

Wednesday 12:03

We have identified some unusual activity on your Online Banking. Log In via the secure link <http://169.239.129.3/personal> to avoid account suspension.

# PUBLIC WI-FI

- May not be trustworthy. They could share your information to other companies who operate in countries without any data protection.
- You may not know who is watching you whilst you're online.

## What to do and not do to

- Don't use online banking. Use your own data.
- Don't conduct any purchases
- Use a virtual private network (VPN)

# JUICE JACKING

USB charging ports in airports, hotels and elsewhere can be replaced with modified versions capable of delivering malware to devices once they're plugged in. An even easier method is modifying an AC adaptor or even a charging cable to do the same thing. This works, of course, because the USB standard is designed to convey both electricity and data. At public charging stations, people are thinking of using USB only for charging, but cybercriminals intend to use it to steal data or for malware delivery.

Do you often charge your mobile device from public ports while travelling? Did you know this can lead to "**Juice Jacking**" ?

## Beware of Juice Jacking

Attackers use USB charging ports available at public places to install malware, steal data or even take complete control of your device.



### Tips to stay safe



Disable data transfer feature on your mobile phone while charging



Get a charge only cable instead of cable supporting charging and data transfer capabilities



Try to carry a power bank



If possible, switch off the device while charging from public ports

Home > Money > Consumer affairs

## Another homebuyer loses £67k as solicitors fail to warn of email fraud



37



First time buyer Howard Mollett transferred more than £74,000 to a fraudster and to date has only received £7,837 back

### FOLLOW TELEGRAPH MONEY

[Follow on Facebook](#) [Follow on Twitter](#)

[Follow on LinkedIn](#)

### Featured Current Accounts (T&C's Apply)

Bank	Account Name	Offer	More details
First Direct	1st Account	Receive £100 Cashback when you switch	<a href="#">Apply</a>
TSB	Classic Account	3% AER on balances up to £1,500	<a href="#">Apply</a>
Natwest	Reward Account	3% rewards on selected household	<a href="#">Apply</a>



Scams

# 'We lost £120,000 in an email scam but the banks won't help get it back'

In another example of a growing menace, the Scotts thought they were sending money to their solicitor's bank account. Little did they know it went to a fraudster



Miles Brignall

Sat 21 Oct 2017 07:00 BST




1,212 | 864



most popular

 Tory MPs' hard Brexit letter to May described as ransom note

 How burnout became a sinister and insidious epidemic

 How rightwing media is already attacking Florida teens speaking out

 Queen makes surprise appearance at London fashion week

 Chronic heavy drinking leads to serious risk of dementia, study warns

Advert

DIGITAL SAFETY

PROMOTED CONTENT

# Email scammers took my house deposit

Hackers are targeting homebuyers and getting away with thousands of pounds

July 23 2017, 12:01am



Hackers trick buyers into sending deposits into their rogue accounts

# PASSWORDS ADVICE

- Use 1 password per account.
- Three random words is The National Cyber Security Centre's advice. Capitals, special characters and numbers is your own choice.
- If you follow this advice your passwords security will be significantly increased against a brute force attack.
- You should change your password frequently.

# THE MOST COMMON TYPES OF MOBILE AD FRAUD TODAY:

1. IVT: Invalid Traffic : Webscrawlers , spiders , bots
2. Check Injection : Click Spamming :when other apps are downloaded and trigger clicks before an install completes. (android devices).
3. Ad Stacking: multiple ads are displayed all at once, one on top of the other. This allows an unscrupulous publisher or other involved partner to say that they technically served an ad and should receive payment for serving said ad, even though the ad was never technically visible.

#### 4. App Spoofing:

(spoofing example **when an email is sent from a false sender address, that asks the recipient to provide sensitive data.**)

Mobile app spoofing occurs **when the app on which the ad impressions is generated is misrepresented.** But instead of sending a fake URL as is the case with domain spoofing, the app sends a fake bundled ID, which is the identifier of the app.

#### 5. Background Ad Activity:

instead of showing a video ad to a real person, the ad is played purely in the background and not seen by anyone. This way, the fraudster can still charge per view, even though no one actually saw the ad.

# ADVICE

In the physical world we're good at protecting ourselves and our property, we need to replicate this in the digital world.

80% of cyber-crime is preventable.

# ADVICE

- Update and migrate
- Activate your firewall
- Spread Awareness
- Data encryption
- User accounts privileges i.e admin
- Cyber insurance
- Prepare Plan

# YOU ARE THE BEST DEFENCE!

## Technology is only a small part of Cyber Defence

- **You are the most important person – protect yourself**
- For businesses/family the most important and best defence is Cyber Security Aware employees – train your staff/family

Always be aware!

Always be on your guard!