



Fraud Awareness

May 2018

Prevalent Frauds types

1. Social Engineering

- Phishing, Vishing

2. Payment Fraud

- CEO Impersonation, Invoice Fraud.

3. Online / Cyber Fraud

- Malware & Trojans, Security Software, Social Networks

4. Get DigiSafe

Social Engineering

- “The manipulation of situations and people that results in the targeted individuals divulging confidential information”



Phishing
(Email)




Vishing
(Telephone)

Phishing – Email Scams

Date: Wed 19/06/2016 10:14
From: ebuy services

Adjustments to your account settings!!!



Account Status Notification

Dear Customer,

We are contacting you to inform you that our Customer Liaison Team has identified changes to your account. In accordance with our User Security Policy we are contacting you to ensure that your account is not fraudulently accessed. Therefore you must access your account using the link below to reactivate your account immediately.

YOU WILL NOT BE ABLE TO ACCESS YOUR ACCOUNT UNLESS YOU DEACTIVATE THIS BLOCK NOW.

Please log in by clicking the link below:

<https://www.ebuy.com/verify/idp.login.html>

Thank you for your help.

Security Officer
Ebuy Online
© Ebuy.com. N.A

<http://www.phishing-scam.com/ebuy.com/verify/idp.login.htm>
Ctrl+Click to follow link

- There are number of email scams in circulation and it's important to remember that this is not a secure channel – emails addresses can be disguised and email accounts hacked
- Phishing is when fraudsters send an email appearing to be from a known organisation asking you to click on a link to a fake website, and ask you to enter your login and password credentials. Fraudsters can then harvest these details to commit fraud
- Alternatively when you click on the link or attachment, malicious software can be downloaded onto your PC which allows fraudsters access to your sensitive information
- There is also more targeted phishing – where fraudsters take the time to research about employees – their role, interests, activities etc to create fake emails to appear to be from an organisation they are familiar with.



Guidance

- Do not click on links/attachments in unexpected emails. Roll your mouse pointer over the link to reveal its true destination.
- If you are unsure, contact the sender directly on a method other than the email you have received.

Phishing emails – some Barclays examples

From: Barclays alerts <ibinfo@alerts.ins.uk>
Subject: Ebanking service message
To: xxxxxxx@gmail.com

Dear Client,

As part of our ongoing commitment to provide the Best Possible online service and protection to all clients, we require you to validate your online access using our safe SSL servers.

[Please confirm profile records](#)

You are required to adhere to this as soon as possible as failure to do so may affect your future online access.

From: Barclays <auto-confirm@amazon.co.uk>
Subject: Errors Were Detected On Your Account

Dear Esteemed Customer,

We are introducing additional security procedures to better protect you when you use our online banking. You are required to activate your account to this service in order to avoid service suspension

[Sign in](#) to complete the process.

To ensure your safety, extra steps have been added to verify your identity.

Regards,
Barclays Online Security Team



Dear Barclays customer,

Due to recent activity on your account we have temporarily blocked access to your account. Barclays protect you when there is sign of suspicions activity on your account. You may be receiving this message because you signed in from a different location or device, if this is the case your access will be restored immediately once you update your security information. [Click here](#)

Thank you for being a valued Barclays customer.

To see all of the Alerts available to you, please log on to www.barclays.co.uk.

From: barclays.co.uk <ib.msg@c.alert.uk>
Subject: Important customer message
To: xxxxxxx@gmail.com

Dear Barclays Client,

An unusual conflict between the card number and profile records associated with your online access was detected therefore certain online features have been deregistered. To restore your online access, kindly update your personal details by following the reference below.

[Confirm online profile details](#)

These features are made to provide the best protection to you as failure to adhere may affect your future online access.

Vishing – Telephone scams



This is when a fraudster calls claiming to be from the 'Fraud team' at your bank or other known organisation. They ask you to confirm confidential information or transfer money to a 'safe' or 'holding' account.

They may even know information about your account such as balances or transactions to convince you they're genuine.

They can disguise the origin of the call through applications faking caller ID - so it displays the number of the service/person they are impersonating helping the deception.



Guidance

- Do not assume a caller is genuine because they have some basic information about your account and don't always trust caller ID – it can be changed
- Barclays will never call and ask you to make a payment or provide bank details to you to make payments
- Barclays will never ask you to allow access to your system.
- If you receive a phone call requesting confidential information, access to your computer or to make payments, verify it is authentic by calling back using contact details held on file or contact your relationship team immediately to verify.

Payment Fraud



CEO Impersonation
Fraud



Invoice Fraud

CEO Impersonation (Business Email Compromise)

- Business email compromise scams are when a fraudster hacks a CEO or a senior employee's email account and sends an email to a colleague requesting a payment to an account which the fraudster is in control of
- Fake email addresses can also be created which are similar to that of the CEO or senior official, and fraudsters can disguise emails as being sent by the recognised sender
- They can also insert fake emails into existing genuine email trails.

Guidance

- Be cautious about any unexpected emails which request payments even if the message appears to have originated from someone within your organisation
- Always check payment requests directly with the member of staff using details held on file to confirm the instruction is genuine
- Employees should check privacy settings on social media and information shared on social networks along with employee information displayed on the organisation's website.



Invoice fraud



- Invoice fraud is when a fraudster impersonates a known supplier or client and sends an instruction advising of new bank account details or requests a payment
- This is usually by email but can be by letter or telephone
- When you go to make your payments to pay invoices for example, these are sent to an account the fraudster controls

Variations seen

- Fraudsters can alter genuine invoices sent in emails from your customer/supplier and amend the beneficiary account details.
- Emails; letters and invoices where payment details are provided for the first payment are also being altered.

Guidance

- Make all staff aware and ensure there is a process in place where you always call your supplier or client, using contact details you have on file, to confirm any change in bank details
- Ensure you validate the exact sort code and account details in full
- Electronic payments are made based on sort code and IBAN number only. Any account name given is not routinely checked. This is the same for all banks and it is the responsibility of the remitter to ensure the account details being used are correct by conducting independent verification.



Malware and Trojans

Malware

- Short for 'malicious software', malware can give the fraudster access to:
 - Personal information
 - Account details
 - Passwords
 - Key logging and mouse movement
 - Watch the victim's screen



Trojans

- Act as 'backdoors' to the affected computer, giving the fraudster remote access.
- Hard to detect as they remain passive when not in use

Ransomware


- Allows the fraudster to gain control of the victim's system and encrypt their files
- Fee is demanded to unlock them

How does Malware get onto your machine?

- Email attachments
- Visiting false or infected websites
- Malicious links on popular websites
- Advertising content on popular websites
- Macros in documents
- External devices (USB, CD etc)
- Physical security breaches
- Fake anti-virus products

Malware Example

From: Barclays Bank PLC [mailto:notification@barclays.com]
Sent: 26 November 2013 13:00
To: Client@emailaddress.com
Subject: Barclays transaction notification #827909

Attachments:  barclays_transaction.zip (5 KB)



Transaction details

Transaction is completed. £2390 has been successfully transferred.
If the transaction was made by mistake please contact our customer service.
barclays_transaction.zip is attached.

Barclays Bank PLC

Barclays is a trading name of Barclays Bank PLC and its subsidiaries. Barclays Bank PLC is authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and the Prudential Regulation Authority (Financial Services Register No. 122702). Registered in England. Registered Number is 1026167 with registered office at 1 Churchill Place, London E14 5HP.



Internet Security

- Protect your computers, devices and/or networks with up-to-date internet security
- Nothing guarantees 100% security – but it makes you a more difficult target

Get Digi-safe



If you think you are a victim to fraud or received a suspicious email that claims to be from Barclays please contact

Barclays Customer Service at **+91 22 6000 7888**,

or contact us on customerservices@barclays.com