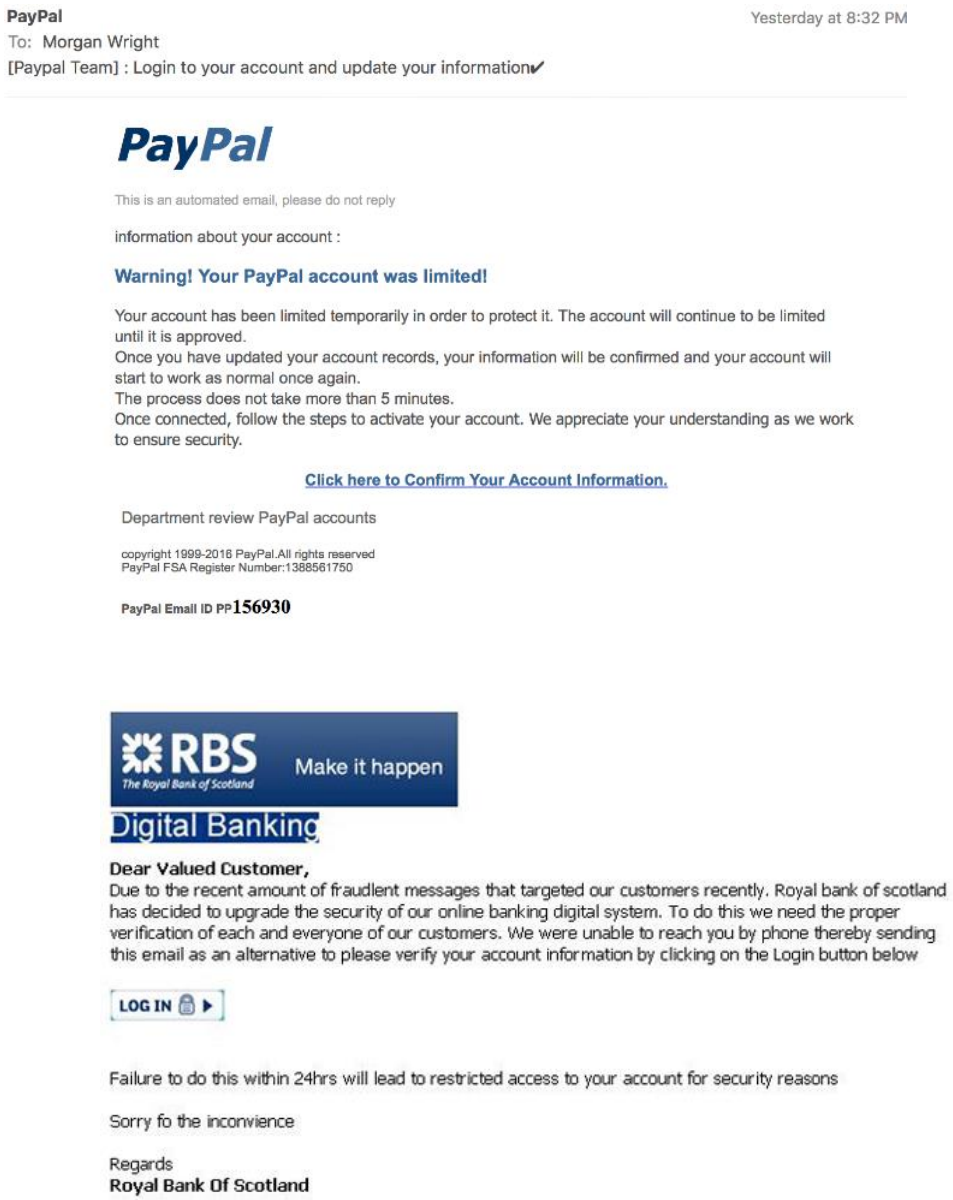
Are your staff trained on cyber-crime? Do they know what a phishing email looks like? Are they aware of the importance of changing their password regularly? Our team of helpful ninjas have provided some useful hints, tips and terminology, to help you, your staff and organisation stay safe:

Terminology:

- **Baiting** – A USB drive or another electronic media device is passed to you, which is pre-loaded with malware.
- **Clickjacking** – Concealing hyperlinks beneath legitimate clickable content, which when clicked, downloads malware.
- **Doxing** – Publicly releasing a person's information, typically retrieved from social networking sites.
- **Cross-site scripting** – When a malicious code is injected into a website.
- **Social Engineering** – A strategic use of conversation to extract information from people without giving them the feeling they are being scammed.
- **Pharming** – Redirecting users from legitimate websites to fraudulent ones for the purpose of extracting confidential information.
- **Phishing** – An email that looks like it is from a legitimate organisation or person, but actually contains a link or file with malware. Avoid clicking on emails that are in your spam folder.
- **Spoofing** – Deceiving computers or users by hiding or faking their identity. Email spoofing utilises a fake email address or simulates a genuine email address.
- **Keystroke logging (Key logger)** – Spyware that is used for covertly recording the keys struck on a keyboard. The log file created by the key logger can then be sent to a specified recipient. By examining the key log data, it may be possible to find private information such as usernames and passwords.

Here are some examples of what phishing emails look like below:



PayPal Yesterday at 8:32 PM
To: Morgan Wright
[Paypal Team] : Login to your account and update your information✔

PayPal

This is an automated email, please do not reply

information about your account :

Warning! Your PayPal account was limited!

Your account has been limited temporarily in order to protect it. The account will continue to be limited 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.
The process does not take more than 5 minutes.
Once connected, follow the steps to activate your account. We appreciate your understanding as we work to ensure security.

Click here to Confirm Your Account Information.

Department review PayPal accounts

copyright 1999-2016 PayPal.All rights reserved
PayPal FSA Register Number:1388561750

PayPal Email ID PP156930

RBS The Royal Bank of Scotland Make it happen

Digital Banking

Dear Valued Customer,
Due to the recent amount of fraudlent messages that targeted our customers recently. Royal bank of scotland has decided to upgrade the security of our online banking digital system. To do this we need the proper verification of each and everyone of our customers. We were unable to reach you by phone thereby sending this email as an alternative to please verify your account information by clicking on the Login button below

LOG IN

Failure to do this within 24hrs will lead to restricted access to your account for security reasons

Sorry fo the inconvience

Regards
Royal Bank Of Scotland

- **Malware** – A buzz word for intrusive software, including computer viruses, Trojan horses and adware.
- **Adware –** Software that automatically downloads or displays advertising banners or pop ups when you are online.
- **Spyware –** Software that enables you to obtain information about another computer's activities by transmitting data using their hard drive.
- **Viruses –** Small programs or scripts that can negatively affect the health of your computer. These malicious programs can create files, move files, erase files, consume your computer's memory and cause your computer not to function correctly.
- **Worms –** A type of virus that replicates itself, but does not alter any files on your machine. However, worms can still create chaos by multiplying so many times that they take up all your computer's available memory or hard disk space. If a worm consumes your memory, your computer will run very slowly and possibly even crash.

- **Trojan Horses –**Software programs that look like regular programs, such as games and even antivirus programs. Once they are run, these programs can do malicious things to your computer.

Password protection hints and tips:

- When creating a new password, it is best to use a mixture of lower case & upper case letters, numbers and unique characters. An example of this would be NiNjABcS3*6#5!
- Change your password on a regular basis and make sure it is different each time. Try not to re-use old passwords.
- Never write your passwords down on paper or save them in your mobile device. If that information gets into the wrong hands, accessing your accounts will be easy.
- While connected to public Wi-Fi, avoid accessing sensitive information which requires password entry. Public Wi-Fi networks are not always protected and your data could potentially be at risk.
- Never provide your password information online or over the telephone. Be aware of suspicious emails which may contain phishing links, trying to access your personal details.

Internet security hints and tips:

- **Out of date security software –** Implementing the latest security software across all of your IT hardware is vitally important. Recent statistics reveal that many companies do not use reliable anti-virus software. To keep your systems clean and free of harmful malware, invest in security software and be sure to carry out regular updates.
- **Vulnerable mobile action plan –** Companies who neglect to implement a secure mobile action plan risk sensitive data being accessed through devices connected to a corporate network. Ask staff to password protect corporate mobile devices.
- **Zero access prevention –** Cyber-criminals are more interested in what's contained in the hardware rather than the hardware itself. Password protect all business devices to prevent unauthorised access.
- **Unsecure Wi-Fi Networks –** Some companies set up their wireless so it shows the network name to those nearby. It may sound obvious, but ensure your Wi-Fi is secure and encrypted to prevent unauthorised access.
- **No firewall security –** Recent statistics reveal that some organisations do not have firewall security. Installing a firewall provides a solid defence against cyber criminals, malware and viruses.
- **Poor data backup schedule –** Sadly, few companies back up their data regularly, which can often result in costly data loss. Regularly back up to ensure your data and sensitive information is protected.

Hints and tips on how to avoid a cyber-attack:

- Set secure passwords and do not share them with anyone.
- Keep your operating system, browser, anti-virus and other critical software up to date.

- Verify the authenticity of requests from companies or individuals by contacting them directly. If you are asked to provide personal information via e-mail, you can contact the company directly to verify this request.
- Pay attention to the URLs of websites you visit. Malicious websites sometimes use a variation in common spelling or a different domain (for example, .com instead of .net).
- Turn off the option to automatically download attachments on your e-mails.
- Be suspicious of unknown links or requests sent through e-mail or text message. Do not click on unknown links, regardless of who the sender appears to be.

Please feel free to call our helpful and knowledgeable team on 01843 572600 if you would like any advice about your current IT requirements, including your security. You can also email us at hello@365itsupport.co.uk – we are always happy to help and provide advice for your IT.