IRM INFORMATION RISK MANAGEMENT
.ALTRAN GROUP

eBook

How to avoid cybercriminals this Christmas

December 2018

INTRODUCTION

With the latest expert predictions on up-and-coming hacking methods in 2019, it has never been more important to stay vigilant during the Christmas period. A 4.2% decline in footfall on the high street compared to 2017 means that shoppers are increasingly using online retailers. Whilst this might be great for grabbing an online bargain, cybercriminals will take try to take advantage of unsuspecting shoppers and businesses with multi-million credit card transactions.

In this short guide, we will make recommendations to keep online shoppers smart and to remind businesses of their responsibility to keep customer data safe.

Contents

BUSINESS ADVICE

DDoS Attacks

During Black Friday, distributed denial-of-service (DDoS) attacks on e-commerce providers increased by over 70%. On Cyber Monday, attacks increased by 109% compared to the average in November [1]. This method of attack is clearly a popular choice for cybercriminals during the Christmas season.

How can organisations overcome or prevent an attack?

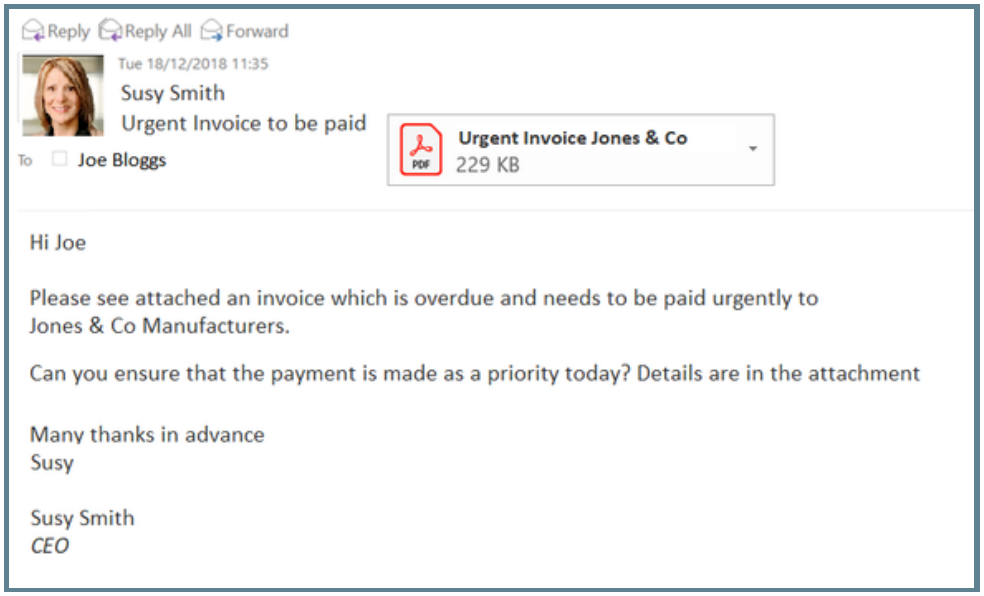
Firstly, invest in infrastructure to try to absorb peak loads. Where possible, invest in cloud-based protection solution in order to counteract targeted attacks. If you don't prepare for attacks of this sort, website downtime could lead to huge **loss of online revenue** and **damage your reputation**.
In addition, many cybercriminals will demand ransom to reinstate your website, potentially costing the business even more money.

[1] https://betanews.com/2018/11/30/ecommerce-ddos-attacks-black-friday/

Employee Reminders

At this time of year, many contracts are ending and purchase orders are being pushed through before business shuts down for Christmas. The constant flow of invoices and other financial documents make it the perfect period for cybercriminals.

Many cybercriminals will target those with financial power in the business. They usually achieve this by falsifying the executive figure's email account and sending authentic-looking emails to other members of staff requesting urgent payments to fake accounts. Whilst these can seem extreme, it is a common occurrence. Just recently, the Save the Children charity admitted to falling victim to a phishing attack last year that cost the business $1m. This was all down to false invoices.



An example of what a fake invoice email could look like.

Consider sending an email to employees to remind them of best practice when it comes to spotting fake emails. Whilst firewalls and email blockers are in place to catch the worst spam emails, employees are ultimately responsible for not clicking on malicious links. Therefore, it is important to ensure they have strong awareness and sufficient training is available on this topic.

CONSUMER ADVICE

Weak Passwords

The most simple rule in the book, yet one that too many people don't abide by.

Statistics gathered this year showed that **almost half of Brits (47%) have either never changed their password, or have only done so in response to a hack.**

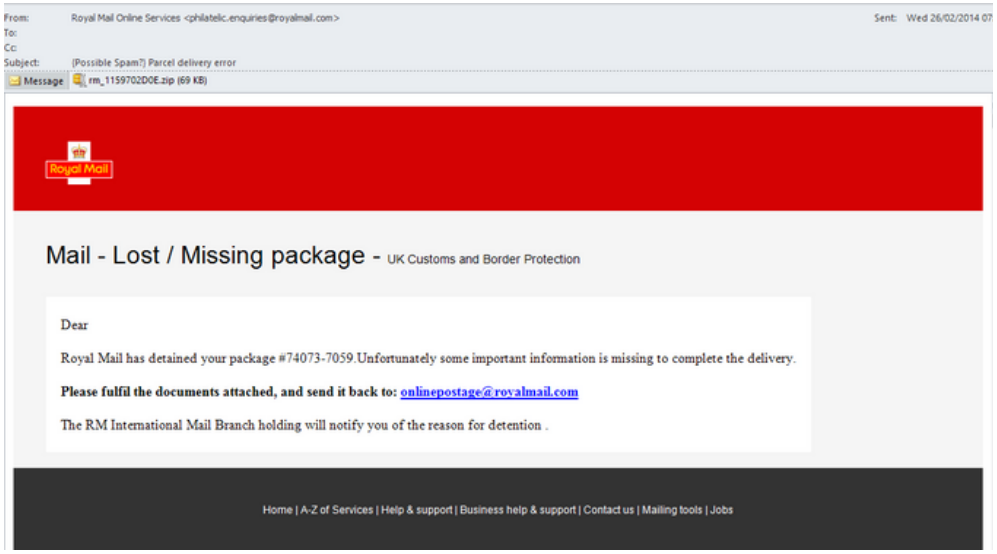
This is worrying considering consumers are more at risk when using the same passwords across multiple accounts. Easily shake this habit by taking a few minutes to set up a password manager and ensure you use **strong** and **separate** passwords.

Software review website, G2Crowd has a **blog on the best recommendations** for free password managers for 2018. The list includes managers such as LastPass and KeePass.

Phishing Emails

For every 10 attempts made by a cybercriminal to infect a device, 9 of them are spam emails [2]. Common spam formats this Christmas include fake delivery notifications or online shopping receipts. The emails involve delivery alerts or purchase information and ask the user to click-through for further details, such as a delivery time. If the user (unfortunately) decides to click-through, it leads them to a website that downloads malicious files to infect the user's system.

A recent test by a cybersecurity firm found that **39% more people clicked on spam emails during the Christmas shopping period** compared to other times of the year.



An example of a malicious lost package 'Royal Mail' email.

[2] https://www.verdict.co.uk/online-shopping-scams-christmas/

The most common malware used by hackers are Emotest, Trivkbot and Panda, which are all designed to capture your banking credentials. Keeping this in mind, remain wary of unusual looking emails asking you to click-through and enter personal details.

Web-based scams to look out for include:

Appealing to your charitable side - scammers impersonating charities asking for 'donations'.

Fake shopping websites – attempting to take advantage of the latest trends by taking your payment but failing to deliver the product (think back to the hoverboard scams of 2016...).

Compromised Twitter accounts - often asking for Bitcoin payment in exchange for a reward. This tactic could be used on a more personal, family-level, such as asking for a loan for presents.

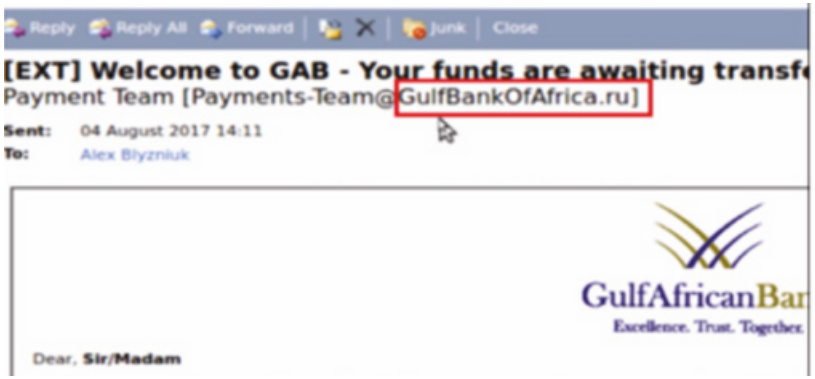
Christmas e-Cards – asking the receiver to click to view the e-Card, which comprises their system and personal details.

5 ways to spot a phishing email:

1. Too good to be true – Received an email offering 80% off everything or free goodies? If it sounds too good to be true, don't be fooled. Make sure you go direct to the website via your browser to check offers rather than clicking on direct links.

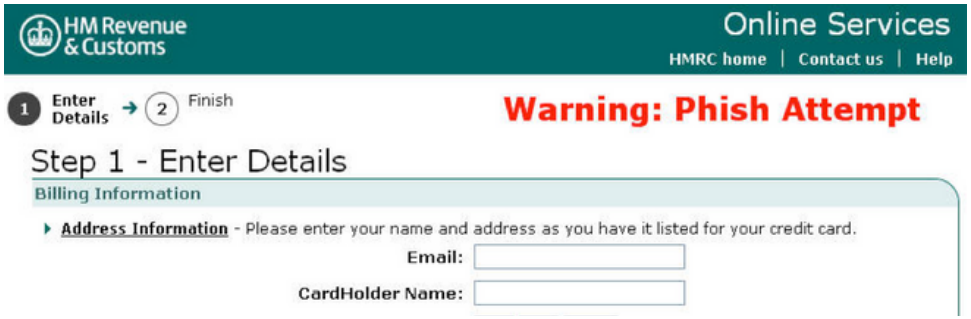
2. Misspellings and bad grammar– Check the email thoroughly for spelling mistakes and unusual grammar. Corporate businesses take pride in ensuring emails go out to customers correctly, so errors can often be a sign of a malicious phishing email.

3. Email domain – Hackers are very clever at making emails appear to be from an official company. If you look into the email sender information in more detail, you are likely to see that the email domain is an elongated or unusual, which is unlikely to match the company name correctly.

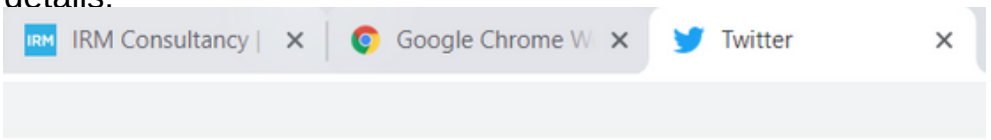


This example shows the email domain doesn't match the company name in the email.

4. Personal details – If an email asks you to enter personal details, especially credit card details, be extremely wary. Equally, if you end up clicking through to a website which requests your personal details, exit the page immediately. Contact the company directly through their official website to double check its authenticity and report the landing page.



5. Images - Keep an eye out for the finer details in emails. Does the logo in the email match the company's usual logo? If you click-through to a landing page, does the little logo (***'favicon'***) appear as an image in the tab? If not, the chances are that the landing page has been quickly drafted as part of a phishing campaign, hence why they've missed the finer details.



This example shows all the legitimate favicons in place on the tabs. If there wasn't a favicon associated with the landing page, it would show a blank piece of paper.

Web Filters

The National Cyber Security Centre (NCSC) has worked hard to **remove almost 140,000 'phishing' websites** used by fraudsters. Whilst this is an impressive effort, malicious websites are still popping up every day. Therefore, it is down to the consumer to recognise what is real and what isn't.

To help you avoid browsing websites that are known to be used for scams, you can install a web filter. A comparison website has highlighted a few web filter options below:

Qustodio

Net Nanny

Surfie

Read the blog from Top Ten Reviews:
https://www.toptenreviews.com/software/security/best-internet-filter-software/

In addition, ensuring you have the latest software and app updates on your computer, laptop and mobile devices will keep you in a more cyber-safe position.

Check bank statements regularly

Last but not least, it's extremely important to keep an eye on your bank statements. Some scams are so sophisticated that you may never realise that you have been a victim.

Keeping a watchful eye on your outgoings will ensure you will notice anything unusual coming out. If something malicious does happen, you will be able to report it to your bank account provider immediately for remediation.

SUMMARY

With all of this said, it's important to reiterate that, whilst cybercrimes do peak around the Christmas period, cybersecurity is a 365 day a year commitment.

Organisations and individuals should educate themselves on cybersecurity all year round. Ensuring you are up to date with the latest software flaws, system malware and scams will allow you to put remediation in place to keep yourself and your business safe and secure.

For further advice speak to us, or visit the National Cyber Security Centre's website for further guidance and tips:
https://www.ncsc.gov.uk/

IRM INFORMATION RISK MANAGEMENT
.ALTRAN GROUP

Learn more about IRM by visiting our website or contacting us directly.

www.irmsecurity.com
hello@irmsecurity.com

SECURE CYBER
UNLOCK OPPORTUNITY