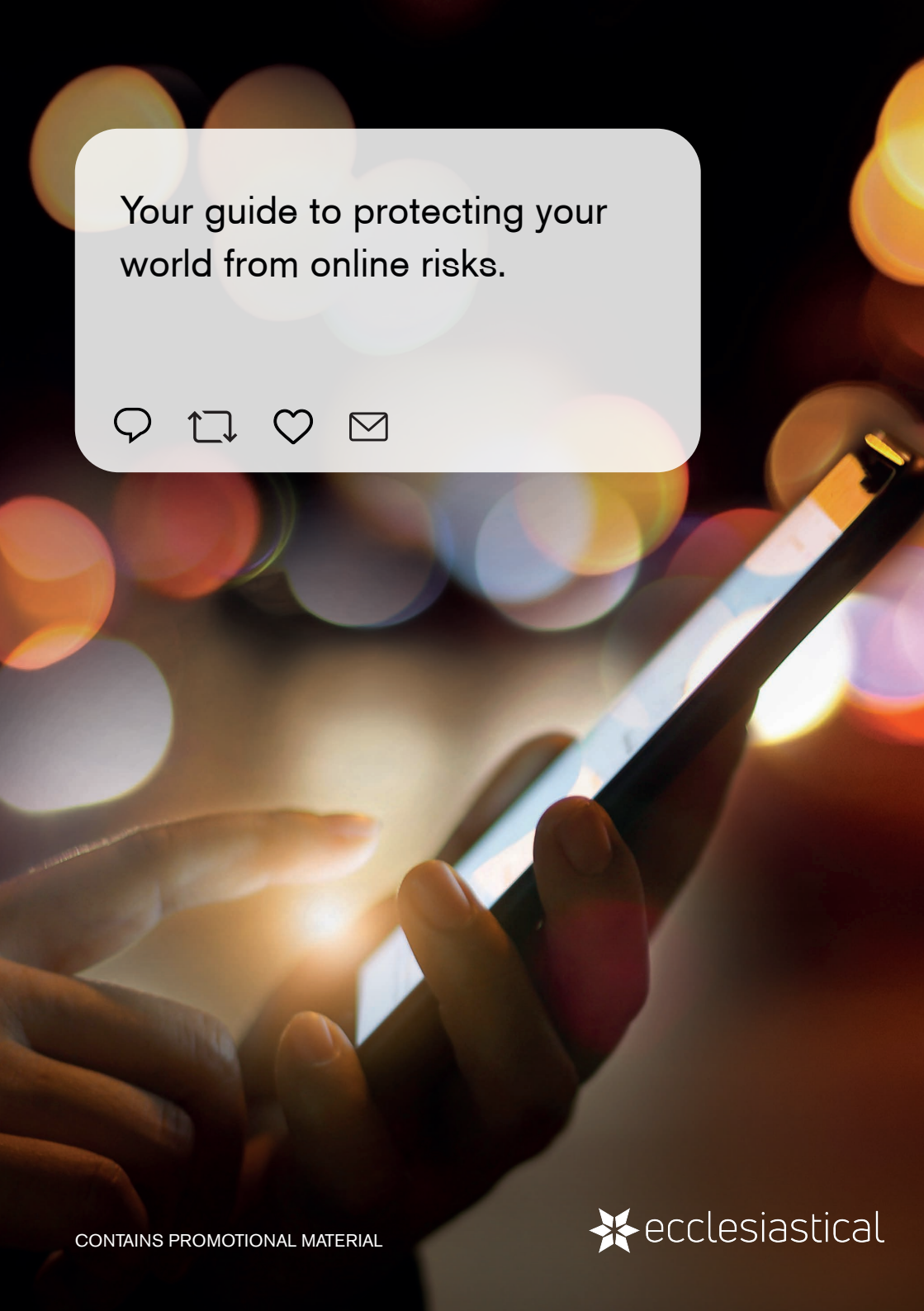



CONTAINS PROMOTIONAL MATERIAL

ecclesiastical

## YOUR GUIDE

Our world, our lives and our homes are increasingly connected. This connectivity has opened the door for previously unimagined opportunity, but with this opportunity comes previously unimagined security risks that affect each and every one of us.

Ecclesiastical continually find new ways to protect the things that are important to you; starting with this simple guide to cyber protection, which is designed to highlight just a few common security issues and solutions to help you manage your online safety with the same scrutiny you'd manage your personal safety.

To help you stay ahead of cyber criminals, we have provided this simple guide.

## WHAT IT COVERS

- Phishing Email
- Spearphishing Attack
- Online Data Sharing
- Home Network Attack
- Dissatisfied Staff
- Man-in-the-Middle Attack.

# PHISHING EMAIL

## Going phishing

**Mark the hacker downloads** thousands of leaked email addresses from the web.

**More than 3 billion phishing emails are sent everyday[1]...** one of them goes to Harriet.

**Harriet receives an email from 'PayPal'** which she happens to use when making online purchases.

## Taking the bait

The email offers a discount if Harriet **logs into her 'PayPal' account** within the next 24 hours. The link redirects Harriet to a fraudulent site.

The fraudulent PayPal site **scans Harriet's computer** and downloads keylogger software that can **record every key stroke made.**

## Identity theft

With banking and online shopping **passwords known to Mark,** he builds up a profile of **Harriet's online identity.**

The PayPal account shows Harriet's bank details, which are used to pay for a number of **online purchases.**

**Harriet's bank account is slowly drained** so it isn't noticed.

Mark is also able to see the details of all of **Harriet's friends and family** in her contacts... **they are also targeted.**

## HOW TO MANAGE THE RISK

Don't store passwords where they can be easily seen – draft emails or notes – **consider password managers.**

**Be suspicious of email discounts or offers.** Always remember that banks will never contact you by email to ask you to enter your password or any other sensitive information by clicking on a link and visiting a website.

If you detect a phishing email, **mark the message as spam and delete it.** This ensures that the message cannot reach your inbox in future.

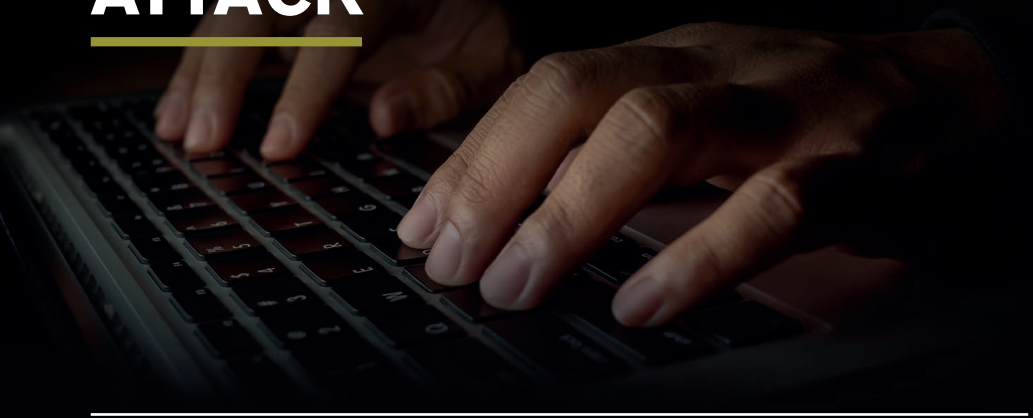
**Never respond to a message from an unknown source.** Take care not to click any embedded links. Phishing emails are sent to a vast number of randomly generated addresses. Clicking embedded links can provide verification of your active email address. Once this occurs it may facilitate the targeting of further malicious emails. Even "unsubscribe" links can be malicious. Ensure that the email is from a trusted source and you are, in fact, subscribed to the service.

Phishing emails will probably contain **odd 'spe11ings' or 'cApitALs** in the sender's email address.

Phishing hackers are unlikely to know your real name, so the email may **address you in vague terms,** e.g. 'Dear Valued Customer'.

[1] www.techrepublic.com 11/06/19

# SPEARPHISHING ATTACK



Mark the hacker is able to research **email addresses and personal information** from social media groups for school parents.

**A well-crafted email is sent to Simon,** one of the parents in the group.

→ Spearphishing time ←

**The email address has been 'spoofed'** to look like the address used by the school's fee payment department.

!!!
Too good to be true

**The email offers a fee discount** for early payment and a link is included.

Mark has created a website **that looks very similar to the school's.**

The discount was too good to ignore, **so Simon transfers the money.**

**The real payment request** comes from the school a week later!

It was a lie

Simon immediately calls his bank, but as he voluntarily sent the money **there's little they can do.**

Simon realises that he might have been the **victim of a scam.**

It has all gone!

Simon has now lost the term's fees for his children and **has to find the extra money.**

## HOW TO MANAGE THE RISK

**The email address** that appears in the 'from' field of an email **is not a guarantee** that the email came from the person or organisation it says it did... **check.**

**Call any known sources by phone,** to check they are bona fide, **if they are asking for money to be transferred.**

# ONLINE DATA SHARING

Jeremy, a local businessman, and his family home are **featured in a national magazine article.**

**Mark the hacker saw the article.** With some research he learnt Jeremy was married with three children and their **social media accounts had limited privacy settings.**

**Mark focused on the son's social media posts,** he was able to find university information and other facts.

His Instagram told Mark that the family went **skiing to the same place every winter.**

This information allowed him to know **when the house would be empty.**

Posts about sports day told Mark which school the children attend. **He was able to confirm patterns and wealth levels.**

**A wealth of information**

**Routines**

Posts about horse riding lessons and other leisure activities **showed when the house was empty during the week.**

Using open source data, Mark was able to find **photographs and the floor plan of the family home.**

**Planning**

In a matter of minutes, Mark has external imagery of the property, **he can see all security features present.**

Mark wants to visit in person... **so he pretends to be a delivery driver,** as the homeowner will open the door every time to one.

After checking the response times of the local police, **Mark picks a time** when Jeremy and his family are away **and breaks in.**

## HOW TO MANAGE THE RISK

**Younger generations** can be the biggest risk to a family's online security, they often overshare information on social media.

Ensure that you and your family have the appropriate privacy settings enabled on your social media accounts. Different social media channels might require **different levels of privacy. Do you know who is following you online?**

**Think twice about posts and photos you're sharing.** Make sure none of your sensitive information is in them – driving licences, passports, letters and other documents. Or posts that show you are on holiday, signalling that your home is empty.

When you enter your details to a website or app, **always check the terms and conditions,** and even then, be careful what you're agreeing to others knowing about you or your account.

Consider the amount of information you give Companies House, **don't use your personal address.**

**Turn off location services** in app settings on your and your children's mobile devices: social media apps, cameras and others that might reveal location. This isn't just about privacy, but also **you and your family's personal safety.**

# HOME NETWORK ATTACK

**John and his family** live in a nice home on a leafy road in the Home Counties.

John's broadband router is **clearly visible in a window.**

Give a hacker an inch and they'll rob you blind...

Mark, the hacker, needs to **get a closer look...**

He waits for an empty driveway and **approaches the house under the guise of a food delivery driver.**

Access to everything

With the router type and password **Mark can easily join it.**

Many of the popular routers have vulnerabilities and the hacker is able **to access all Wi-Fi run devices in the home and monitor their web traffic.**

It's all gone!

When John checks his online bank account he sees that his money has been **transferred to an unknown source!**

## HOW TO MANAGE THE RISK

Check with your broadband provider that the core software or firmware on the router is **the latest version.**

**Ask how to disable WPS** (Wi-Fi Protected Setup), it was supposed to be an easy way to get devices connected to a router. But the push-a-button-to-connect system came with flaws and some routers use the same default digits.

**Remove password** from back of router.

If you use Wi-Fi signal boosters, **check how they connect to your network.**

**Change any factory passwords** on your smart home devices.

Keep your broadband router **out of sight** so the password or device is not visible.

Consider smart doorbells to **capture who visits your home** when you are not in (but don't announce that you are not in).

# DISSATISFIED STAFF

**Harry moves** into his new property.

New home

As Harry's new home is much larger than his previous property, **he needs more domestic staff.**

**Harry speaks to his friends** and they recommend a new housekeeper who is available.

As Harry is a shrewd businessman, he haggles over the desired salary and hours. **The housekeeper eventually accepts and commences work at the house.**

Frustrations

After 6 months, **the new housekeeper becomes disinterested** in working for Harry and is very **unhappy with her current salary and working hours.**

A simple **recording device** bought online for only £10 is hidden in Harry's study by the housekeeper who is now able to **listen in remotely on all conversations in the room.**

Eavesdropping

After months of recordings, **the housekeeper has insight into Harry's business deals** including a large contract that Harry's business is pitching for.

The housekeeper **sells the information** about the large contract to one of Harry's competitors for a large sum of money.

**Harry's rivals use the information** to undercut the contract and they are successful in winning the business.

## HOW TO MANAGE THE RISK

Watch out for domestic staff that keep **strange hours or if they appear disinterested in their work.**

If you are recruiting outside of an agency, **always obtain references for new staff,** but also call their previous employer.

**Consider online searches** to see if the prospective staff member shows up in any online stories or news articles.

# MAN-IN-THE-MIDDLE ATTACK

James, a local homeowner, enjoys the 'café culture' in his village and likes **to visit the busy local coffee shop regularly.**

It's Saturday morning and James **walks to his local coffee shop to use the free Wi-Fi** to complete a few tasks he couldn't quite get to during his busy week.

**Coffee & work**

James buys a coffee and sits down and **gets his laptop out.**

Mark the hacker has created a **fake Wi-Fi network** with a very legitimate sounding name...

**Everyone loves FREE Wi-Fi**

**James logs on** to the fake Wi-Fi network.

**Mark can now see everything** that James does online.

**Man-in-the-middle**

Mark can now monitor James's online activity as he's placed himself in the middle of the connection so is **able to intercept login details, bank card information and more.**

*******

**James's identify and credentials have been stolen** and he's lost money and will face certain distress and inconvenience.

**Identity stolen**

## HOW TO MANAGE THE RISK

**Use your mobile device's data** instead of public Wi-Fi, purchase a bigger data plan if needed **– a mobile cellular signal is secure** as there is no wireless network in between you and the internet.

If you need to log onto public Wi-Fi, then consider purchasing a VPN. They are approximately £80 per annum.

(Virtual Private Network - an arrangement whereby a secure, apparently private network is achieved using encryption over a public network, typically the internet.)

Top 5 VPNs
(according to techradar.com)

- ExpressVPN
- NordVPN
- IPVanish
- Hotspot Shield
- Surfshark.

To find out more, talk to your insurance broker or visit our website **www.ecclesiastical.com/cybersafety**



BLACKSTONECONSULTANCY™

With thanks to Blackstone Consultancy for their involvement in the creation of the guidance.
**www.blackstoneconsultancy.com**

ecclesiastical

Ecclesiastical Insurance Office plc (EIO) Reg. No. 24869. Registered in England at Benefact House, 2000 Pioneer Avenue, Gloucester Business Park, Brockworth, Gloucester, GL3 4AW, United Kingdom. EIO is authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and the Prudential Regulation Authority. Firm Reference Number 113848.

PD3396