NI Cyber Security Centre

Cyber Security

SMALL CHARITY GUIDE

Improve cyber security within your charity

www.nicybersecuritycentre.gov.uk

TABLE CONTENT

CYBER SECURITY **FOR SMALL CHARITIES**

Charities are becoming increasingly more reliant on IT and technology and as a result of this are falling victim to a range of malicious cyber threats.

The recent DSIT Cyber Security Breaches Survey showed that 1 in 5 charities in the past 12 months have fallen victim to a cyber attack. With 83% of those charities citing phishing as a form of cyber attack.*

Cyber criminals do not care if you are a charity or a business. They simply want to exploit any organisation that holds sensitive data or attack for financial gain. If you do not have strong cyber security practices in place you are at risk of being a target for cyber criminals.

This guide will provide you with useful tips for free and easy steps that you can implement to help reduce your risk of cyber attack by the most common cyber threats.

*

BACKING UP YOUR DATA

Think about how much you rely on your charity's critical data, supporter details, information on beneficiaries, volunteer data, governing documents, as well as invoices and payment details. Now imagine how long you would be able to operate without them.

All charities should take regular backups of their important data, and make sure that these backups are recent and can be restored. By doing this, you're ensuring your charity can still function following the impact of flood, fire, physical damage or theft. Furthermore, if you have backups of your data that you can recover quickly, your charity will be more resilient to cyber crime.

Tip 1: Identify what data you need to back up

Identify your essential data. This is the information that your charity couldn't function without. This could include documents, emails, contacts, legal information, calendars, financial records and supporter or beneficiary databases; most of which are only kept on your computer, phone, tablet or network.

Tip 2: Keep your backup separate from your computer

Whether it's on a USB stick, a separate drive or a separate computer, access to data backups should be restricted so that they:

- are not accessible by all staff or volunteers
- are not permanently connected to the device holding the original copy

Ransomware can often move to attached storage automatically, which means any such backup could also be infected, leaving you with no backup to recover data from. For more resilience, you should consider storing your backups in a different location. Cloud storage solutions are a cost-effective and efficient way of achieving this

Tip 3: Consider the cloud

You've probably already used cloud storage during your work and personal life without even knowing - unless you're running your own email server, your emails are already stored 'in the cloud'. Using cloud storage means your data is physically separate from your location. Service providers can supply your charity with data storage and web services without you needing to invest in expensive hardware up front. Most providers offer a limited amount of storage space for free, and larger storage capacity for minimal costs to charities.

4: Read NCSC cloud security guidance

Not all service providers are the same, but the market is reasonably mature and most providers have good security practices built-in. By handing over significant parts of your IT services to a service provider, you'll benefit from specialist expertise that smaller charities may struggle to justify in terms of cost. Before contacting service providers, you should read the NCSC's Cloud Security Guidance. This guidance will help you decide what to look for when evaluating their services, and what they can offer.

Tip 5: Make backing up part of your everyday business

The majority of network or cloud storage solutions now allow you to make backups automatically. Eg, when new files of a certain type are saved to specified folders. Using automated backups saves time and also ensures that you have the latest version of your files should you need them. Many off-the-shelf backup solutions are easy to set up, and are affordable. When choosing a solution, you'll also have to decide how much data you need to back up, and how quickly you need to be able to access the data following an incident

PROTECTING YOUR **CHARITY FROM MALWARE**

Malicious software (malware) is software or web content that can harm your charity. The most well-known form of malware is viruses, which are self-copying programs that infect legitimate software.

Tip 1: Install (and turn on) antivirus software

Should be used on all computers and laptops. For your office equipment, you can pretty much click 'enable', and you're instantly safer. Smartphones and tablets may require a different approach and if configured in accordance with the NCSC's End User Device guidance, separate antivirus software might not be necessary.

Tip 2: Prevent trustees, volunteers or staff from downloading dodgy apps

You should only download apps for mobile devices from manufacturer-approved stores (Google Play or Apple App Store). These apps are checked to provide a certain level of protection from malware. You should prevent charity personnel from downloading third party apps from unknown vendors/sources. Staff accounts should only have enough access required to perform their role, with extra permissions only given to those who need it.

Tip 3: Keep all your IT equipment and software up to date (patching)

For all your IT equipment, make sure that the software and device(s) operating system are always kept up to date. Applying these updates is one of the most important things you can do to improve security. Operating systems, programs, phones and apps should all be set to 'automatically update' wherever this is an option. At some point, software and device suppliers will end their support for older models and updates will no longer be available, at which point you should consider replacing them with modern alternatives.

Tip 4: Control how USB drives (and memory cards) can be used

It is tempting to use USB drives or memory cards to transfer files between organisations and people. However, it only takes one person to accidently plug-in an infected device (such as a USB drive containing malware) to cause lasting damage to your charity's assets and good reputation. When drives and cards are openly shared, it becomes hard to track what they contain, where they've been, and who has used them. You can reduce the likelihood of infection by:

- blocking access to the physical ports (eg USB ports) on the devices being used
- using antivirus tools
- only allowing approved USB drives and memory cards to be used within your charity - and prohibiting their use in other devices (such as home computers)

Make these directives part of your charity's policies and procedures, to prevent it being exposed to unnecessary risks. You can also ask trustees, volunteers or staff to transfer files using alternate means (such as by email or cloud storage), rather than via USB.

Tip 5: Switch on your firewall

Firewalls create a 'buffer zone' between your own network and external networks (such as the Internet). Most popular operating systems now include a firewall, so it may simply be a case of switching this on

KEEPING YOUR SMARTPHONES AND TABLETS SAFE

Mobile technology is now an essential part of life, with increasing amounts of data being stored on tablets and smartphones. These devices are now as powerful as traditional computers, and because they often leave the safety of the office (and home), they need even more protection than 'desktop' equipment.

Tip 1: Switch on password protection

A strong PIN or password will prevent the average criminal from accessing your phone. Many devices now include fingerprint or facial recognition to unlock your device. However, these features are not always enabled when you first receive your devices, so you should always check they have been switched on.

Tip 2: Make sure lost or stolen devices can be tracked, locked or wiped

Trustees, staff and volunteers are more likely to have their devices stolen (or lose them) while out of the office or their home. Fortunately, the majority of devices include free tools that are invaluable should you lose your device. They can help you to:

- Track the location of a device
- Remotely lock access to the device (to prevent anyone else using it)
- Remotely erase the data stored on the device
- Retrieve a backup of data stored on the device

Setting up these tools may seem daunting at first, but by using mobile device management software, you can set up your devices to a standard configuration with a single click

Tip 3: Keep your device up to date

It is important that all your devices are kept up to date. All manufactures release regular updates that contain critical security fixes to keep the device protected. This process is quick, easy, and free; devices should be set to automatically update, where possible. Ensure your trustees, staff and volunteers know how important these updates are, and explain how to do it, if necessary. At some point, manufacturers will discontinue their support for older devices, at which point you should consider replacing them with a newer model or version

Tip 4: Keep your apps up to date

All the applications that you have installed should also be updated regularly. These updates will not only add new features, but will also fix any security issues that have been discovered. Make sure trustees, staff and volunteers know when updates are ready, how to install them, and that it's important to do so straight away

Tip 5: Don't connect to unknown

When you use public Wi-Fi hotspots (for example in hotels & coffee shops), there is no easy way to find out who controls the hotspot, or to know if it’s secure. If you do connect to these hotspots, somebody else could access:

- what you're working on whilst connected
- your private login details that many apps and web services maintain whilst you're logged on

The easiest precaution is to not connect to the Internet using unknown hotspots, and instead use your mobile 3G, 4G or 5G mobile network, which will have built-in security. This means you can also use 'tethering' (where your other devices share the 3G/4G connection from your phone), or a wireless 'dongle' provided by your mobile network. You can also use Virtual Private Networks (VPNs), a technique that encrypts your data before it is sent across the Internet. If you're using third party VPNs, you'll need the technical ability to configure it yourself, and should only use VPNs provided by reputable service provider

USING PASSWORDS TO PROTECT YOUR DATA

Your charity's laptops, computers, tablets and smartphones will contain a lot of important and sensitive data such as the personal information of your beneficiaries and supporters, as well as details of your online accounts. It is essential that this data is available to you, but not available to unauthorised users. Passwords - when implemented correctly - are a free, easy and effective way to prevent unauthorised users accessing your devices.

Tip 1: Make sure you switch on password protection

Set a screenlock password, PIN, or other method (such as fingerprint or face unlock on your mobile devices). If you're mostly using fingerprint or face unlock, you'll be entering a password less often, so consider setting up a long password that's difficult to guess. Make sure that your office equipment (laptops and PCs) all use an encryption product (such as BitLocker). Most modern devices have encryption built in, but you'll need to ensure it's turned on and configured.

Tip 2: Use two step authentication for 'important' accounts

Enable two-step authentication (2SA) on your accounts. It adds a large amount of security for not much extra effort. 2SA requires two different methods to 'prove' your identity before you can use a service, generally a password plus one other method. This could be a code that's sent to your smartphone that you must enter in addition to your password.

Tip 3: Avoid using predictable passwords

Using strong passwords is an important way to protect your charity's valuable data. Make sure trustees, staff and volunteers are given advice on setting secure passwords that is easy for them to understand. Passwords should be easy to remember, but hard for somebody else to guess. A good rule is to use three random words to create a strong password. Avoid using the most common passwords, which criminals can easily guess (such as P4$$w0rd or QWERTY).

Your charity's IT systems should not require trustees, volunteers or staff to share accounts or passwords in order to get their job done. Make sure that every user has personal access to the right systems, and that the level of access given is always the lowest needed to do their job whilst minimising their access to systems they don't need to use. This will lower the risk of wider damage if a user downloads malicious software (like a virus).

Tip 4: How to cope with 'password overload'

Only enforce password access to a software or system if you really need to. Where you do use passwords to access a service, do not enforce regular password changes. Passwords really only need to be changed when you suspect a compromise of the details. People will forget passwords, so make sure they can reset their own passwords easily. Consider using password managers, which can create and store passwords for you that you access via a 'master' password. Since the master password is protecting all of your other passwords, make sure it's a strong one, eg by using three ran by using three random words.dom words.

Tip 5: Change all default passwords

One of the most common mistakes is not changing the default passwords that smartphones, laptops, and other types of equipment are issued with. Change all default passwords before devices are distributed within your charity. You should also check devices and software regularly to detect unchanged default passwords

AVOID
PHISHING ATTACKS

In a typical phishing attack, scammers send fake emails asking for sensitive information (eg bank details), or containing links to bad websites. They might try to trick you into sending money, steal your details to sell on, or they may have political or ideological motives for accessing your charity's information. Phishing emails are getting harder to spot, and some will still get past even the most observant users. Whatever the size and nature of your charity, you will receive phishing attacks at some point.

Tip 1: Configure accounts to reduce the impact of successful attacks

You should configure your charity's IT systems in advance using the principle of 'least privilege'. This means giving trustees, staff and volunteers the lowest level of user rights required to perform their role, so if they are the victim of a phishing attack, the potential damage is reduced.

To further reduce the damage that can be done by malware or loss of login details, ensure that your personnel don't browse the web or check emails from an account with Administrator privileges. An Administrator account is a user account that allows you to make changes that will affect other users. Administrators can change security settings, install software and hardware, and access all files on the computer. An attacker having unauthorised access to an Administrator account can be far more damaging than accessing a standard user account.

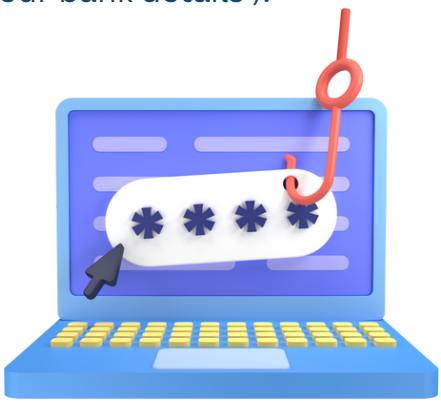
Use two step authentication (2SA) on your important accounts such as email. This means that even if an attacker knows your passwords, they still won't be able to access that account.

Tip 2: Think about how you operate

Consider ways that someone might target your charity, and make sure your trustees, staff and volunteers all understand normal ways of working, so that they're better equipped to spot requests that are out of the ordinary. Common tricks include sending an invoice for a service that you haven't used, so when the attachment is opened, malware is automatically installed (without your knowledge) on your computer. Another common scam is to trick staff into transferring money or information by sending emails that look authentic. Think about your usual practices and how you can help make these tricks less likely to succeed. For example:

- Do trustees, staff and volunteers know what to do with unusual requests, and where to get help?
- Ask yourself whether someone impersonating an important individua via email should be challenged (or have their identity verified another way) before action is taken.
- Do you understand the day-to-day relationships your charity has? Scammers will often send phishing emails from large organisations (such as banks) in the hope that some of the email recipients will have a connection to that company. If you get an email from an organisation you don't do business with, treat it with suspicion.
- Develop training material to help encourage and support people in your charity to question suspicious or just unusual requests, even if they appear to be from important individuals. Having the confidence to ask ‘is this genuine?’ can be the difference between staying safe, or a costly mishap.

You might want to access how your outgoing communications appear. For example, do you send unsolicited emails asking for money or passwords? If so your emails may get mistaken for phishing emails, or leave people vulnerable to an attack that's been designed to look like an email from you? Consider telling your trustees, staff and volunteers what they should look out for (such as 'we will never ask for your password', or 'our bank details').



Tip 3: Check for the obvious signs of phishing

Expecting your trustees, staff and volunteers to identify and delete all phishing emails is an impossible request due to how sophiscated phishing emails have become. However, many phishing emails still fit the mould of a traditional attack, so look for the following warning signs:

- Many phishing scams originate outside the UK and often the spelling, grammar and punctuation are poor. Others will try and create official looking emails by including logos and graphics. Is the email what you'd expect from a credible, large organisation?
- Is it addressed to you by name, or does it refer to 'valued customer' etc? This can be a sign that the sender does not actually know you, and that it is part of a phishing scam.
- Does the email contain a a sense of urgency? Be suspicious of words like 'send these details within 24 hours' or 'you have been a victim of crime, click here immediately'.
- Look out for emails that appear to come from a high-ranking person within your organisation, such as a trustee or manager, requesting a payment is made to a particular bank account. Look at the sender's name and double check the email address. Does it sound legitimate, or is it trying to mimic someone you know?
- If it sounds too good to be true, it probably is. It's most unlikely that someone will want to give you money, or give you access to some secret part of the Internet

Tip 4: Report all attacks

Make sure that your trustees, staff and volunteers are encouraged to ask for help if they think that they might have been a victim of phishing, especially if they've not raised it before. It’s important to take steps to scan for malware and change passwords as soon as possible if you suspect a successful attack has occurred.

Do not punish staff if they get caught out and create a blame culture. It discourages people from reporting in future, and can make them so fearful that they spend excessive time and energy scrutinising every email they receive.

Tip 5: Check your digital footprint

Cyber Criminals use publicly available information about your charity and staff to make their phishing messages more convincing. This is often taken from your website and social media accounts.

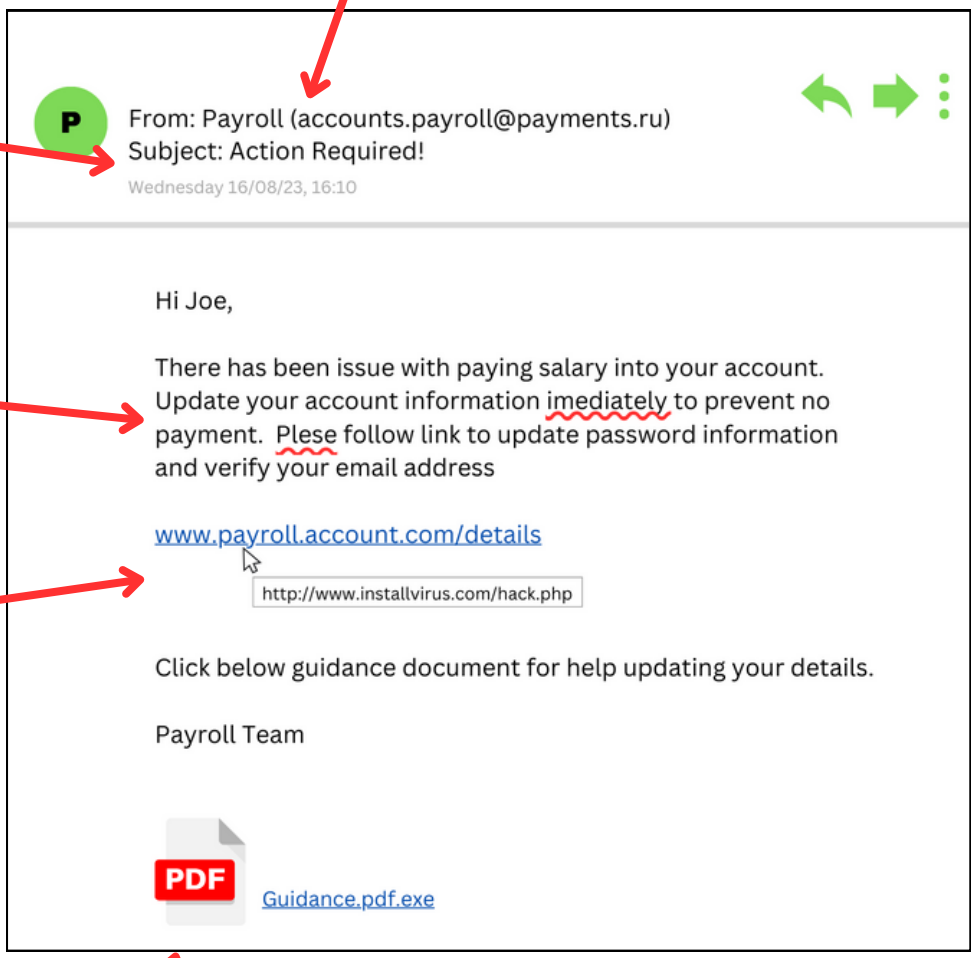
- Understand the impact of information shared on your charity's website and social media pages. What do visitors to your website need to know, and what detail is unnecessary (but could be useful for cyber criminals)?
- Be aware of what your trustees, staff and volunteers give away about your charity online.
- Help your staff understand how sharing their personal information can affect them and your charity. This is not about expecting people to remove all traces of themselves from the Internet. Instead support them as they manage their digital footprint, shaping their profile so that it works for them and the charity.

EXAMPLES OF PHISHING EMAILS

Phishing emails are getting more sophisticated. In this guide we have provided some tips on what to look out for;

Email Address - Look at the details of this account - It has come from a Russian address

A sense of **urgency**

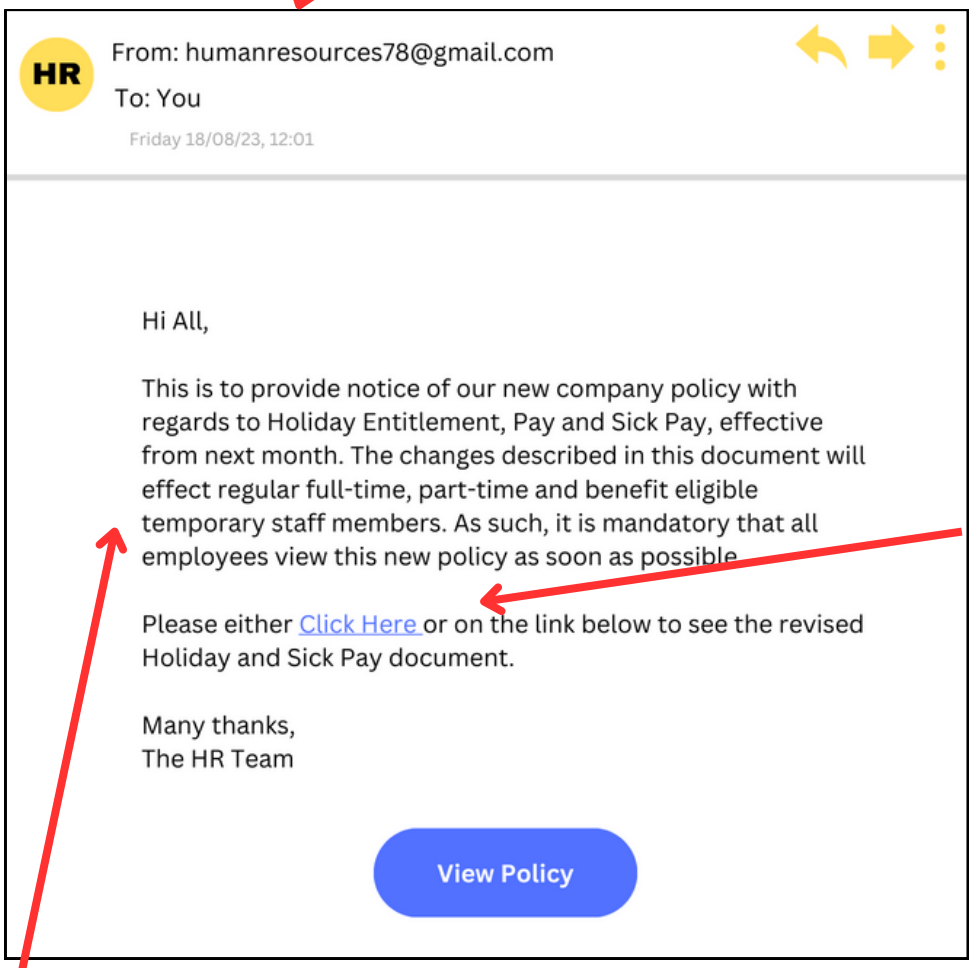


Spelling and grammar mistakes

Suspicious link that doesn't match the destination

Unexpected attachments - especially files ending in .exe

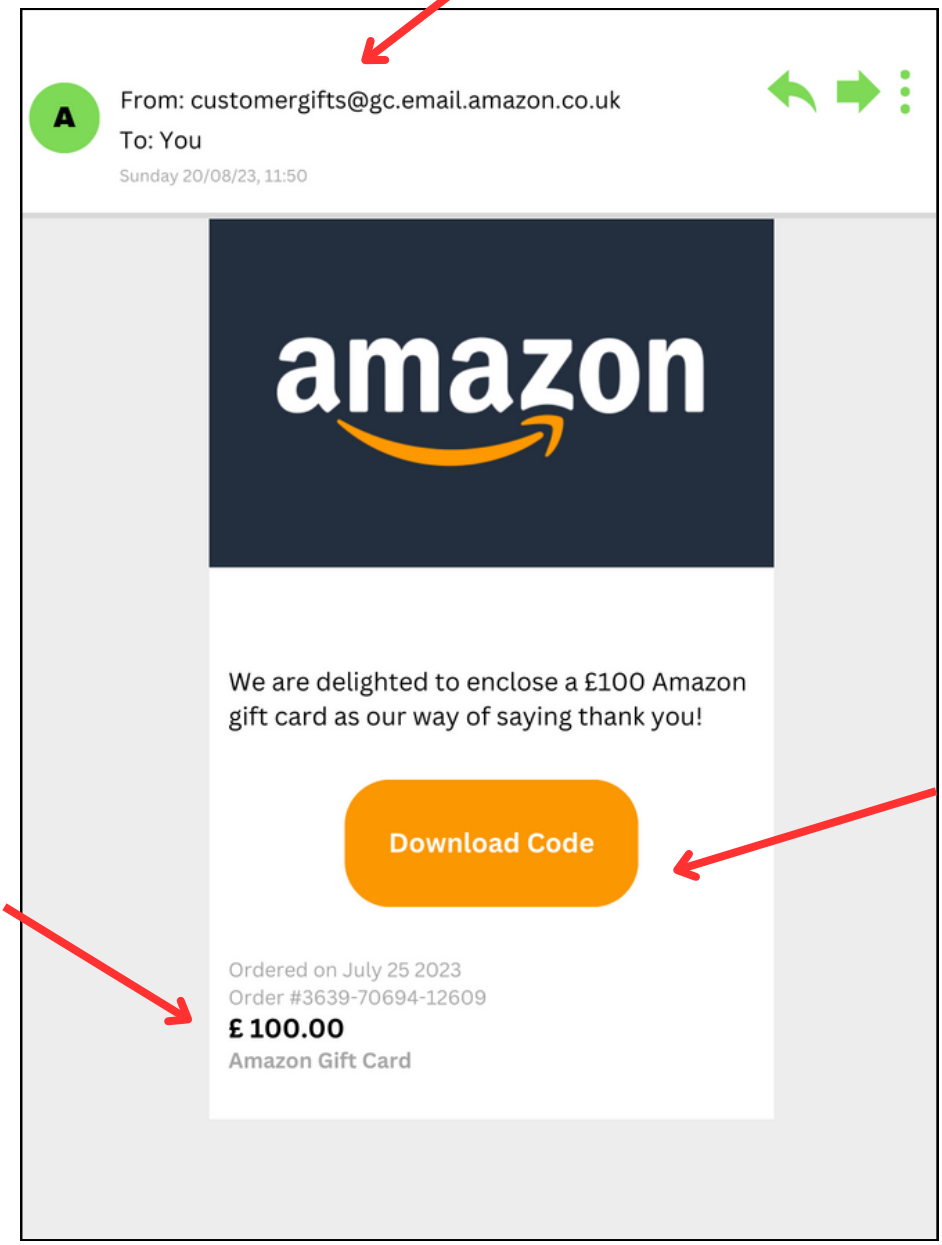
Email Address - Look at the details of this account - having a number in the address and using a gmail account should raise suspicion



Link included in email - these links will direct you to a fake webpage where cyber criminals can steal your date or infect your device/network with virus's etc.

Content of email - The content in this email will trick people into clicking the link due to it relating to holiday and pay. Two topics that will be of high interest to your employees.

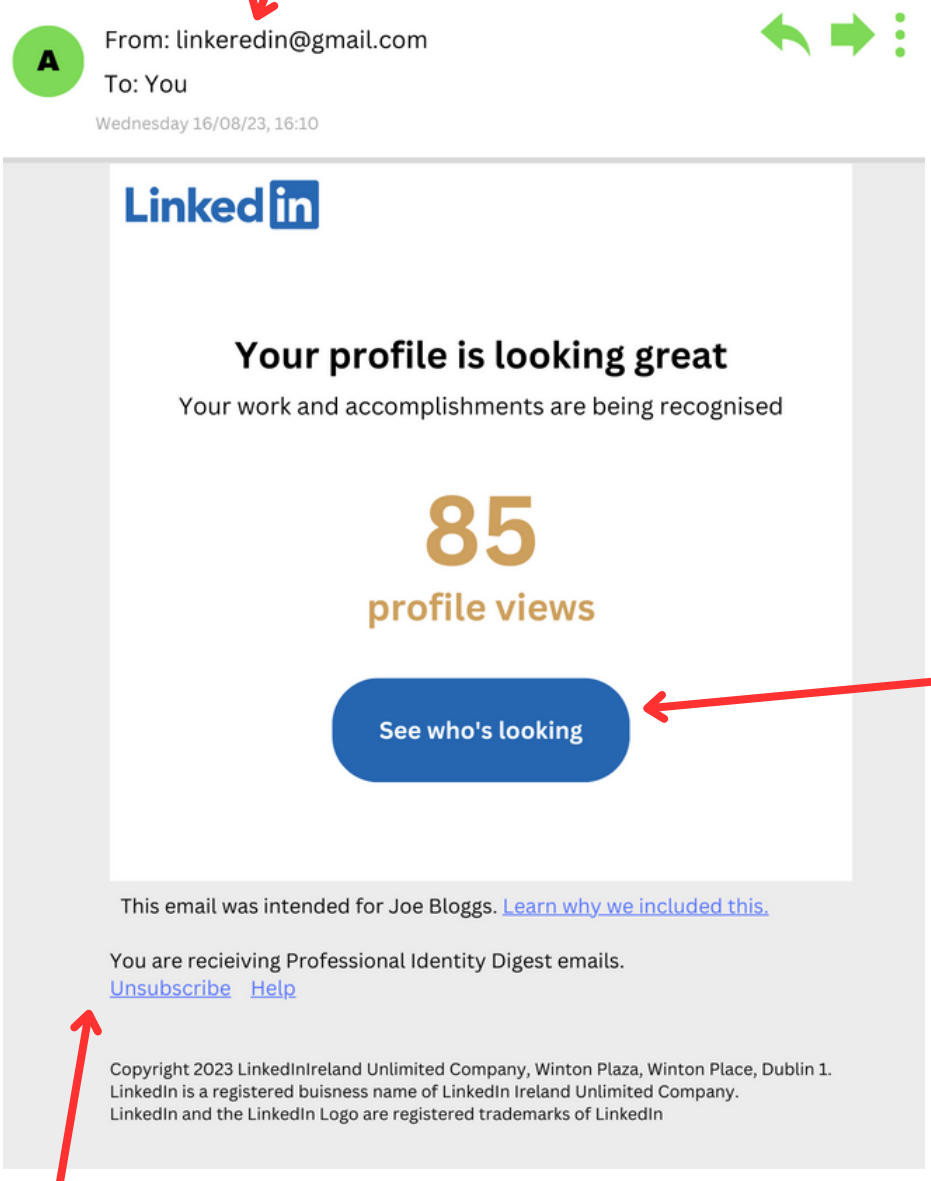
Email Address - Isn't an official Amazon email - Always click on the senders name to check the email address



Link included in email - these links will direct you to a fake payment webpage where cyber criminals will steal your card information when you enter the details

Offer of money - If it is too good to be true, it most likely is.

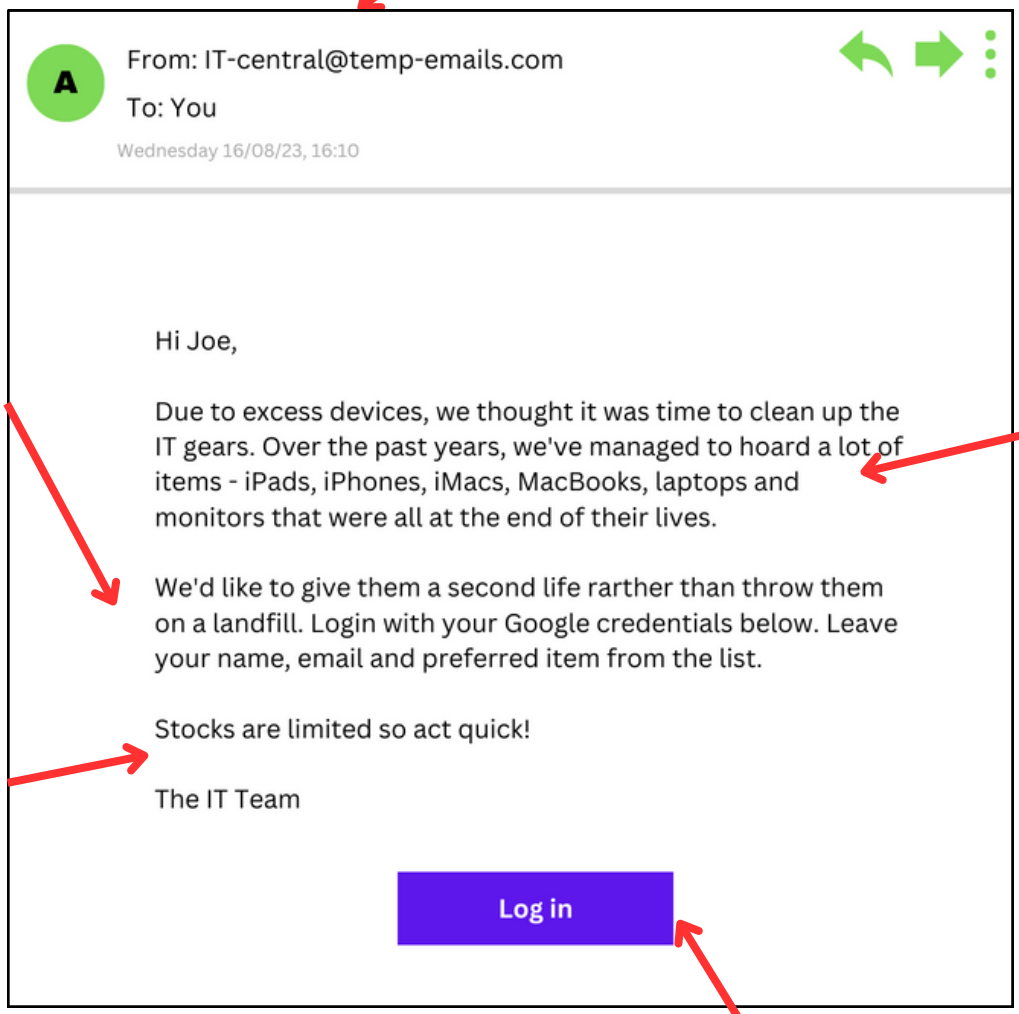
Email Address - Look at the details of this account - LinkedIn is spelt wrong as has come from a gmail account. This should raise suspicion as has not come from an office LinkedIn email address



Link included in email - these links will direct you to a fake webpage where cyber criminals can steal your date or infect your device/network with virus's etc.

Content of the email - This sentence doesn't match up to what the email is relating to. This email is promoting your to go to LinkedIn to see who is looking at your account. However, further down the email it states you are receiving 'Professional Identity Digest' emails.

Email Address - Is this an email address you know? It looks suspicious due to the sender using a 'temp-email' provider



Email is asking you to log in with your google credentials which is suspicious

The offer of high end tech items seems too good to be true - It is.

Urgency - Limit stock gives a sense of urgency that if you don't click the link soon you could lose out

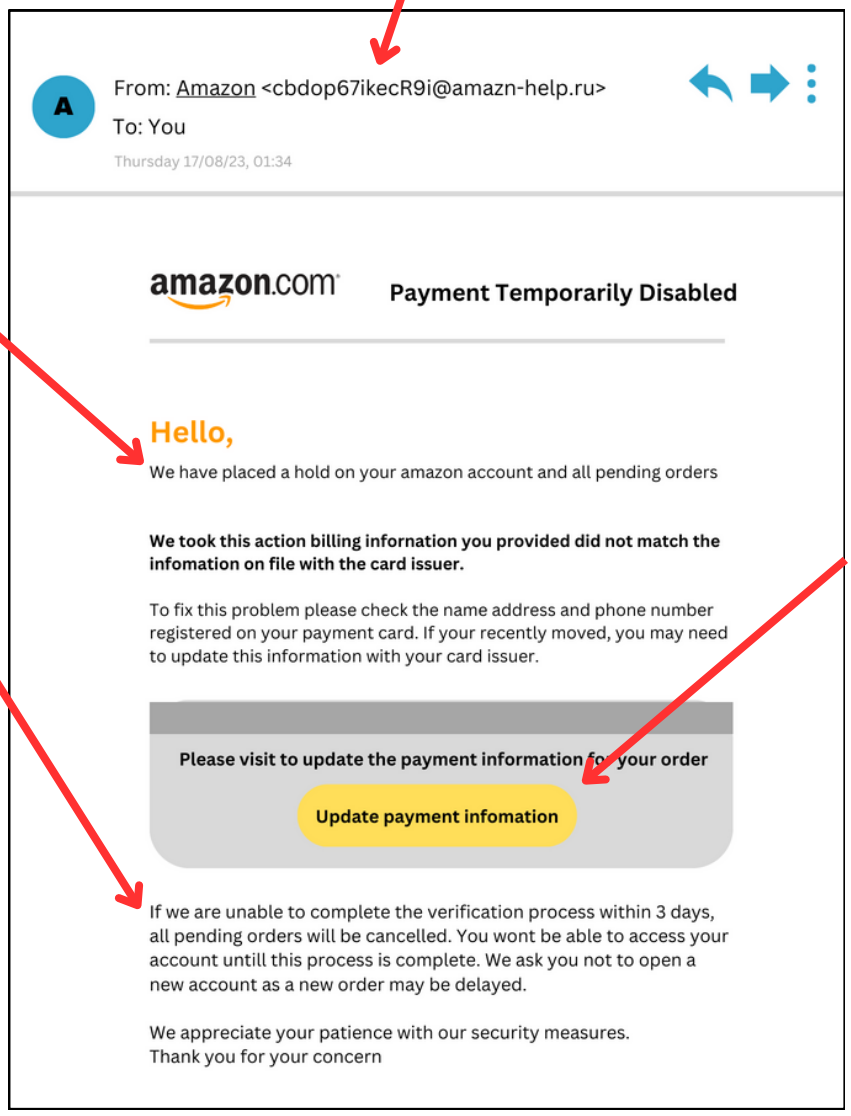
Link included in email - these links will direct you to a fake payment webpage where cyber criminals will steal your card information when you enter the details

Email Address - Doesn't match sender name - Always click on the senders name to check the email address. The '.ru' at the end of an email address tells us that this is a Russian account.

Pressure - Account put on hold disabled

Urgency - you have 3 days to update details before all pending orders are cancelled

Link included in email - these links will direct you to a fake payment webpage where cyber criminals will steal your card information when you enter the details



www.nicybersecuritycentre.gov.uk
info@nicybersecuritycentre.gov.uk

NI Cyber Security Centre