HOW TO AVOID EMAIL SCAMS

THE TECH TEAM

Technology Made Easy

HOW TO AVOID EMAIL SCAMS

They're sneaky, sinister, and they can be dangerous. Email scams are unfortunately very common, and it's important that you know how to avoid them - and how to get yourself out of a potentially sticky situation if you do fall for one.

Below, we've outlined some of the most common email scams.

The 'Wealthy Person' Scam:
An allegedly wealthy person or family asking if they can relocate a large sum of money from their bank account to yours. They ask you to confirm your bank details by paying a small fee - and then they'll disappear, keeping the money that you've paid.

How to Avoid it: If you're sent an email from somebody you don't recognise, proceed with caution. If somebody is asking you to share or send them personal information, it's very likely that it's a scam. Delete the email straight away, without replying or clicking on any links.

AN INTRODUCTION TO GOOGLE WORKSPACE

The 'Spoofed Email' Scam:
A 'spoofed' email is one that a scammer sends pretending to be somebody else. While the email might look legitimate, the content of the email may seem suspicious. For example, they may ask for money or for you to confirm personal details. They'll then harvest and sell this data.

How to Avoid it: When 'spoofing' an email, the sender uses a fake email address to make their email look more trustworthy. Make sure to check who an email is really from by clicking on the sender's email. If it's fake, the email address will be different. For example, it might change from a legitimate-looking email like 'admin@natwest.co.uk' to the more suspicious 'john_12@457684.com'. If you don't recognise the sender, don't click on any links - and delete the email straight away.

The 'Credit Loan or Bank Details' Scam:
An email that informs you that you've been pre-approved for either a credit card or loan, or that you need to update your bank details. They might ask you to click a website link, or to send them personal information. They'll then harvest and sell this data.

How to Avoid it: If a company or your bank is getting in touch with you regarding your finances, it's usually only after you've contacted them first. If you receive an unsolicited email, this should be a red flag. Legitimate comp

YOU SHOULD NEVER PROVIDE YOUR DETAILS TO A SENDER YOU DO NOT KNOW

“I THINK I’VE BEEN SCAMMED - WHAT DO I DO?”

Firstly - don’t panic! If you think you may have been scammed, try to keep calm, and seek some advice.

If you’ve transferred money to a scammer:
If you’ve done this within the last 24 hours, contact the police straight away on the 101 non-emergency number. They’ll be able to help.

If you think your bank details may have been stolen:
Contact your bank straight away. They’ll be able to protect your account. After you’ve told them, keep an eye on your transactions in case of any suspicious activity.

If you think a password has been stolen or your account was hacked:
Change your password straight away, and log out of all accounts if you’re able to use this option. If you use the same password on multiple accounts, change your password on there too. Make sure it’s a strong password, including uppercase and lowercase letters, numbers, and special characters - such as ‘!’ or ‘?’.

If you have any other concerns, you can report a scam email by contacting Action Fraud or The National Cyber Security Centre.

6 GOLDEN RULES TO STAY SAFE

1. **Is the Sender, actually the sender?**
   If you are at all suspicious about an email, check the FROM addres to see if it has been “spoofed”.
2. **Is the email addressed to you?**
   If the email is not personalised, for example it is addressed to Dear Sir/Madam or something obscure like that, you should be wary of the content. Businesses must have your permission to contact you these days and often anything that isn’t personal could just be “spam”.
3. **Are you being hurried into action?**
   If the subject suggests urgency - be wary! Ring the company and check if in doubt.
4. **Are there any obvious spelling or grammar errors?**
   Look for grammatical and spelling errors in the content.
5. **Don’t click on any links or log in to your accounts from suspicious emails:**
   You can always check the links before you click by hovering over them and identifying the true destination (URL/Website).
6. **NEVER respond to an email asking you to update or re-enter personal or bank details.**
   Should you receive an email requesting this, contact your bank immediately and they will assist you.

FURTHER HELP

"What a comfort to know that when confusion strikes Jonny and his team and friendly, approachable and available to rescue the situation. Good value for money."

- Julie & Kevin

★★★★★

Technology problems? We can help! TheTechTeam is the first and last stop for people who are a bit baffled by modern technology. Our experts have many years of experience working with customers of every skill level to simplify all the technical jargon and provide the best solution to each individual's needs from repair, to advice and support.

Get in touch with us today and let us know how we can help you!

0191 209 9088
www.thetechteam.it
hello@thetechteam.it

THE TECH TEAM
Technology Made Easy

0191 209 9088 | www.thetechteam.it