visionict.com

Website Design | Surveys | Graphic Design | Data Backup | Training & Support

Implementing good ICT security strategy and practices

nalc

National Association of Local Councils

Our four pillars

Collaboration

We take pride in forming long lasting relationships with our clients

Longevity & Support

Our priority is our clients

Honest Pricing

Open and transparent, we'll find the right option for you

Social Responsibility

Supporting local charities, organisations and social enterprises

Is your data, website & emails safe?

Cyber security is about protecting your computer-based equipment and information from unintended or unauthorised access, change, theft or destruction.

Getting the basics right

General

Always download software updates –

They contain vital security upgrades that will keep your device and information safe.

With open source websites such as WordPress it is vital to do this to ensure security.

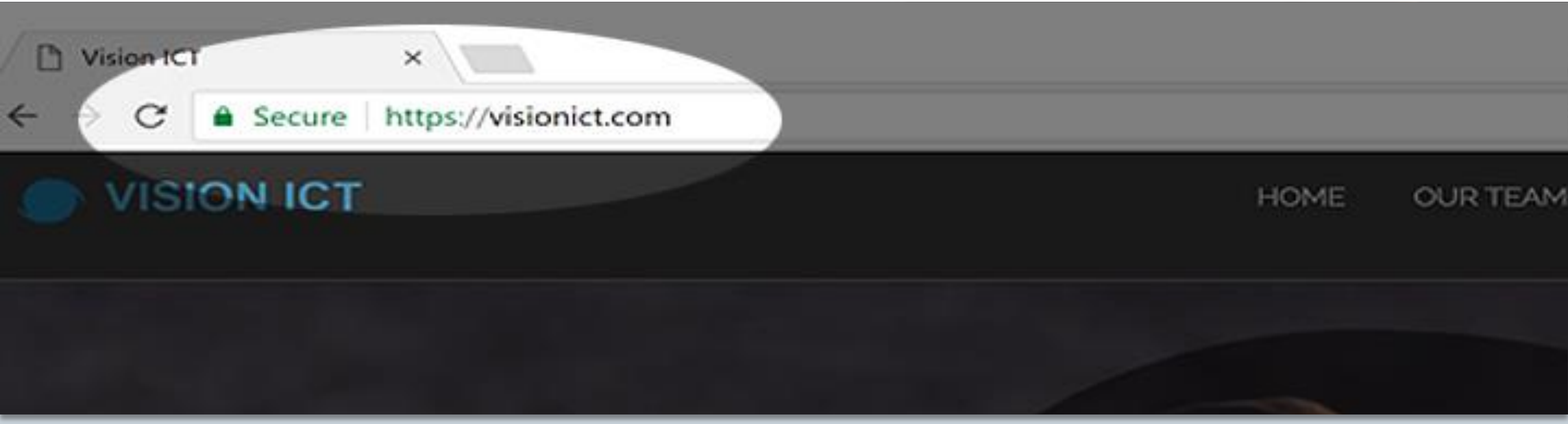
Use anti-virus software

Computers, tablets, smart phones can easily become infected by small pieces of software known as viruses or malware.

You do need to install internet security software like anti virus on all your devices to help prevent infection and **ensure these are kept up to date**.

Websites: SSL Certification

SSL Certificates are small data files that digitally bind a cryptographic key to an organisation's details. When installed on a web server, it activates the padlock and the https protocol and allows secure connections from a web server to a browser. Typically, SSL is used to secure credit card transactions, data transfer and logins, and more recently is becoming the norm when securing browsing of social media sites.

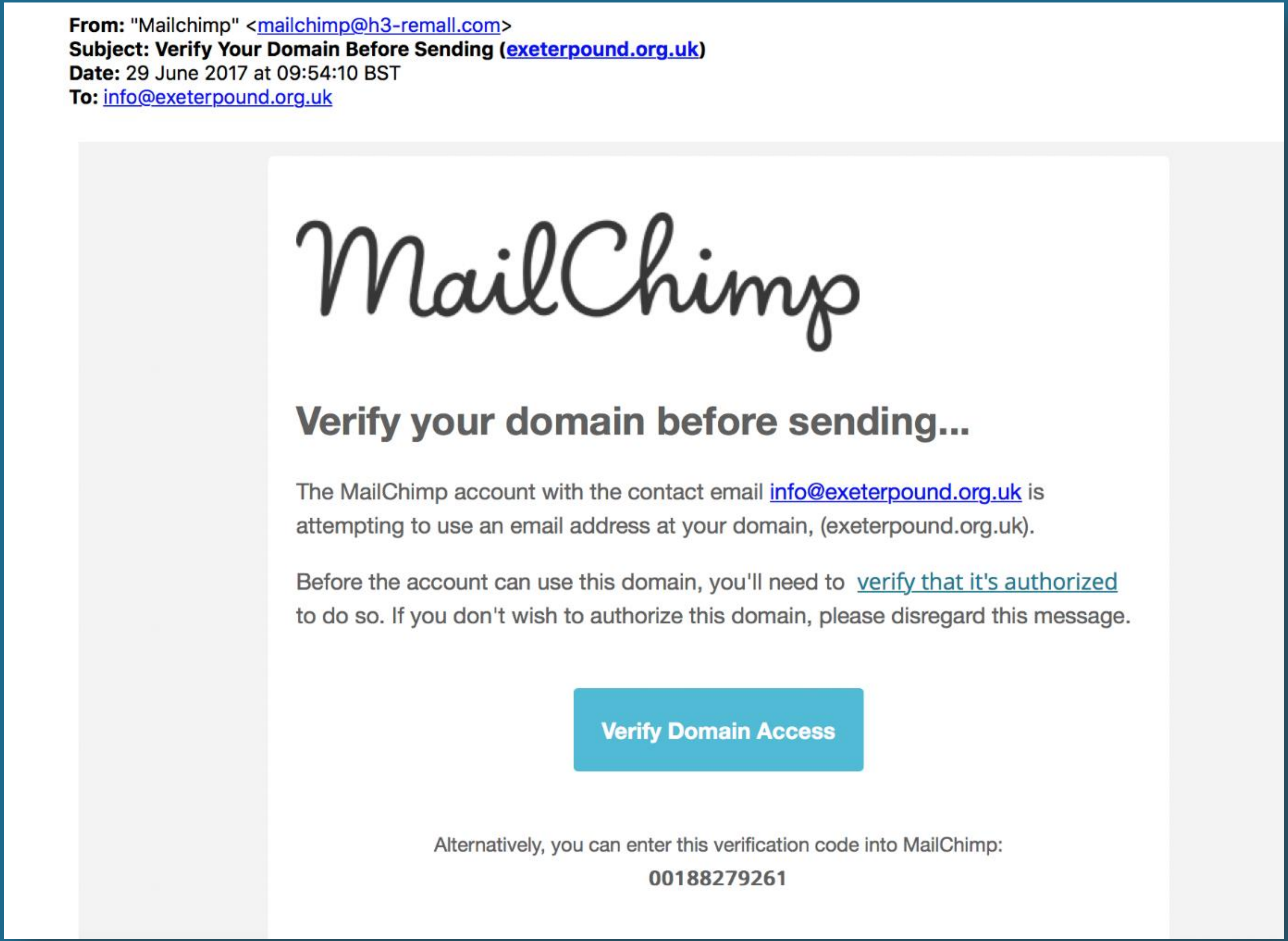


Use of passwords

- Strong passwords – Use 2 random words at least 8 characters, upper and lower case letters, numbers and symbols.
- Do not use the same password for everything.
- Do not leave them lying around your office or home.

Email

- Delete and never open suspicious emails.
- Never give out account information requested through an email or open links to sites which may well have viruses and fraudulent requests for information.



From: "Mailchimp" <mailchimp@h3-remall.com>
Subject: Verify Your Domain Before Sending (exeterpound.org.uk)
Date: 29 June 2017 at 09:54:10 BST
To: info@exeterpound.org.uk

MailChimp

Verify your domain before sending...

The MailChimp account with the contact email info@exeterpound.org.uk is attempting to use an email address at your domain, (exeterpound.org.uk).

Before the account can use this domain, you'll need to verify that it's authorized to do so. If you don't wish to authorize this domain, please disregard this message.

Alternatively, you can enter this verification code into MailChimp:

00188279261

Backing up your data

Check that your website is being backed up

Computer files need to be backed up hourly or at least daily

- If stored on a hard disc place in a safe location away from the computer.
- USB sticks - how often do you loose these?
- Automatic back up with off site storage is cheap and easy these days.
- So easy to get distracted and not manually back up data.

Don't let this be you:

> ***"I was about to but ……"***
> *The worst happens when you least expect it.*

So what is at risk?

- All your information.
- Files, accounts, letters, posters and images.
- Your reputation.

Who will put you at risk?

Simply anyone or anything!

- Fire or theft.
- An ex employee.
- A teenager learning their hacking skills.
- A visitor who sees a password lying around.
- Someone probing for access to your IT system.
- Increasingly, professionals from around the world.

What is the impact

Your time ! Your money

Planning – Implementing - Reviewing

- If you are a council of more than just one employee, then you need to ensure that all employees and Councillors are committed to cyber security.
- Identify what the risks are. Plan a clear strategy which everyone can follow to ensure that your council is not put at risk.
- On this basis write up your Council's Strategy for this and implement agreed actions.
- Train staff: do they know what their responsibilities are? Do they know what good practice looks like.
- If you are attacked or something goes wrong how will you deal with it?
- Keep it simple, ensure it is clear.
- Review regularly.

Questions

Sharing good practise