South Thames
Colleges Group

Cyber Security Policy

July 2023

RAD Volo

CYBER SECURITY POLICY

1. Introduction

Cyber security is how staff at South Thames Colleges Group can work together to help reduce the risk of a cyber-attack on the organisation. Cyber security's core function is to protect the devices we all use (laptops, computers, tablets and smartphones), and the services we access with them from malicious attacks. It's also about preventing unauthorised access to the information we work with on a daily basis.

South Thames Colleges Group is fully committed to operating a safe and secure IT environment as part of its Cyber Security response, we provide security through our network firewall and through the use of anti-virus software, along with a range of other tools and preventative measures. However, these measures cannot catch every threat and STCG rely on you being alert to threats and taking due care to avoid them.

2. Types of Cyber Attack

There are mainly two types of attack know as **Phishing** and **Ransomware**.

Phishing is an attempt by criminals to steal information. Phishing emails try to trick you into disclosing sensitive personal or financial information such as your login name and password, your credit card details or your bank account details.

The criminals send you an email hoping to fool you into responding, typically by directing you to a website where you are asked to provide confidential, personal or financial information. The email appears to come from an organisation known to you (e.g. Fedex, Apple) or even from an internal source such as IT Services. Note that phishing emails can also lure you to open suspicious attachments or visit websites that can infect your computer with malware.

How do I recognise a Phising attack?

- False Sense of Urgency – Many scam emails tell you that your account will be in jeopardy if something critical is not updated right away.
- Spelling and grammar mistakes – Often these emails contain multiple spelling or grammar mistakes or look unprofessional.
- Fake Links – The email may contain links that look genuine but are not. Check where a link is going before you click by hovering your mouse over the link in the email, and comparing it to the link that is actually displayed. If the link looks suspicious, don't click on it.
- Invalid sender email address – Bear in mind that the sender can disguise their email address to make a fake address seem genuine.
- Generic greeting – Phishing emails will often greet you as “Dear email user” or similar.
- Attachments – The vast majority of organisations will never send you unsolicited attachments or software. You should never open an attachment unless you are 100% sure it comes from a legitimate source.

Ransomware – a type of malware which ‘locks’ the files on a computer and then demands payment to unlock them – is a seriously growing threat all across the world, with many examples of successful attacks in Education.

Ransomware attacks are launched via email and are a major threat to our data. They have the potential to cause reputational damage and loss of important data.

How do I recognise a Ransomware attack?

Ransomware is typically delivered via an email which asks you to open an attached file which contains the Ransomware virus. The email may look genuine in many respects and may seem to come from a bona fide source (e.g. Fedex). Remember that email addresses can be 'spoofed' to disguise their true source.

Many Ransomware emails have had the following subject lines:

- Invoice
- Unable to deliver your parcel
- Purchase order
- You have a new voicemail

You should take extra care with emails with these subject lines but also be aware that the attacker could use any subject which might hope to attract your attention.

Ransomware emails have attachments which they will encourage you to open. You should be vigilant about all attachments even from known sources, as they may well have already been compromised. You should only open an attachment if you are expecting one from a known source and you are satisfied that the email is genuine.

3. Key questions to ask yourself before responding to an email

- Am I expecting this email?
- Do I know the sender? If you don't recognise the email address, this is a warning sign that you shouldn't ignore.
- Are there red flags (Impersonal greeting, Spelling mistakes, Unusual fonts)?
- Displayed email address in address bar and actual address sent from do not match?
- Does the email contain an unusual request?
- Have I actually purchased or used the service being referred to?
- Does the message ask for any personal information (password, credit cards, etc)?
- Does the message ask for sensitive information about others?
- Does the message ask you to immediately open an attachment?

If the answer to any of these is "no" then you should delete the email or at the very least verify its authenticity.