Types of Cyber Threat

Attacks can come in a wide variety of forms. They can be very targeted towards a handful of individuals right the way across to a whole business or multiple businesses. Understanding these attacks is the first step towards securing yourself.

The identity of the attacker is often unknown

Users often don't know they've been hit until it's too late

Malware

Malware is one of the most common threats to businesses and home users alike, and can cause devastation if it successfully infects and spreads in a company. Malware is a computer program thats sole purpose is to damage infrastructure, spy on company matters, steal sensitive files, or lock all data and hold the organisation to ransom. The latter is called Ransomware. The ways malware can infect is through email, malicious sites, infected documents, adverts on website, and more.

Phishing attacks

Be wary of emails and documents that ask you to send sensitive information such as usernames and passwords. If an employee falls for the cat and mouse trick, malware can infect the company's infrastructure and cause harm. It is important to educate your employees to identify an email that looks illegitimate, and doesn't come from a trusted source. Many of the emails will have errors in them, which is done on purpose, to filter out the smart from the gullible.

Social Engineering attacks

An attacker may choose to attack your business through social engineering your employee. This can be in the form of spear phishing emails, a phone call, in-person conversation and more. The former is the most common attack. Social engineering a person is to try and trick them into giving over sensitive information without them realising it. For example, an attacker might send an email to an employee that poses as their superior, asking them to change their login password as they haven't done it in a while - by clicking on the attacker's malicious link.

Distributed Denial of Service Attack (DDOS)

DDOS is a common attack that is aimed to flood the target with connections to overload their website or their network. This brings down the company's services and causes great disruption, and in the end, tries to stop the business from being able to operate.

//curious frank:

www.curious-frank.com

A division of the Scottish Business Resilience Centre