12 email threats quick guide

Spam
Spam is unsolicited bulk email messages, also known as junk email. Spammers typically send an email to millions of addresses. Used to distribute malware and phishing attacks and loads servers.

Brand or Domain Impersonation
Brand or domain impersonation is a type of cyber attack in which an attacker creates a fake domain, social media account or email that appears to be affiliated with a legitimate brand or organisation.

URL Phishing
Phishing is when criminals try to trick users into providing sensitive information. URL phishing is a type of phishing attack in which attackers create fake websites that mimic the appearance of legitimate sites.

Blackmail
Blackmail scams, including sextortion, are increasing in frequency, becoming more sophisticated and bypassing email gateways. Criminals leverage usernames and passwords stolen in data breaches.

Scamming
With email scamming, cybercriminals use fraudulent schemes to defraud victims or steal their identity by tricking them into disclosing personal information ie fake job postings, and fund transfers.

Business Email Compromise
In BEC attacks, scammers impersonate an employee in the organisation in order to defraud the company, targeting employees, customers, or partners with access to the company's finances.

Malware
Malware is a type of software that is designed to harm, infect, or take control of a computer system or network without the user's knowledge or consent. ie viruses, worms, Trojans, ransomware and spyware.

Conversation Hijacking
Conversation hijacking, also known as "session hijacking", is a type of cyber attack in which an attacker intercepts and takes control of a communication session between two parties to eavesdrop.

Data Exfiltration
Data exfiltration refers to the unauthorised transfer or theft of data from a computer or network to an external location or destination via email, file transfer protocol (FTP), cloud storage or removable USB's.

Lateral Phishing
With lateral phishing, attackers use recently hijacked accounts to send phishing emails to unsuspecting recipients, such as close contacts in the company and its partners, to spread the attack.

Spear Phishing
Spear phishing is a type of targeted phishing attack that is designed to deceive a specific individual or group of individuals, typically for financial gain or to gain access to sensitive information.

Account Takeover
Account takeover is identity theft and fraud, where a malicious third party successfully gains access to a user's account credentials using, phishing brand impersonation and social engineering.

For a more detailed guide visit www.mpsplc.co.uk/services/cyber-security/