Malware and spam: Phishing emails

This article reviews **what spam and phishing are**, as well as **how to protect yourself**.

> **See also:**
>
> - Malware & Spam: Ransomware

Spam

What is it?

Spam is **unsolicited email**. Much like physical junk mail, spam can simply be **deleted** or **ignored**. Microsoft 365's Online Protection features automatically identify and block spam emails – but **no anti-spam solution is perfect**!

Common methods to look out for

> **Never download an unknown attachment!** Attackers will include malware that infects your device.

- Advertising an **item or service** to purchase
- Advertising a **cause** to support
- Convincing you to download an **attached file**

How to block it

Microsoft 365's Online Protection features automatically identify and block spam emails – but **no anti-spam solution is perfect**!

- **Do not respond** to unknown senders
- Mark items as Junk
- Report particularly sophisticated messages to the Help Desk
- Be aware of what sites are **asking for your College email**

Phishing

What is it?

Phishing consists of emails sent with the purpose of **gaining personal information**. This information is then used to **compromise account(s)** and, in turn, send out similar messages to other unsuspecting recipients.

Common methods to look out for

Email spoofing is quite common – allowing attackers to be disguised as **known companies** or **users**.

- **Threatening** or **aggressive** language
- **Time-sensitive** actions
- Convincing you to **click a link** or **reply**

I think I'm compromised!

1. Change your password
2. Contact the Help Desk

If you encounter this issue outside of Help Desk hours, call the Help Desk when it opens or email help@brynmawr.edu.

Questions?

If you have any additional questions or problems, don't hesitate to reach out to the **Help Desk!**

Phone: 610-526-7440 | Library and Help Desk hours⧉
Email: help@brynmawr.edu | Service catalog⧉
Location: Canaday Library 1st floor