43% of cyberattacks happen at SMBs[1]

Here are some simple things you can do to protect yourself and your colleagues.

91% of cyberattacks start with a phishing email[2]

Shield your company from email threats:

- Verify senders—hover your cursor over the "From" name to see what address pops up (make sure the two match).
- Don't click on links or attachments unless you've verified the sender.
- Don't click a link without hovering your cursor over it to see if the URL that pops up matches the intended site.

58% of users accidentally share sensitive information[3]

Take care of customer information:

- Use only encrypted tools with controlled user access, like Microsoft SharePoint, Teams, or OneDrive, to send and store confidential data.
- Protect customers' GDPR-protected personally identifiable information, like Social Security numbers and medical info.
- Limit access to confidential information to users who truly need it.

81% of hacking breaches use compromised credentials[4]

Protect yourself by creating strong passwords:

- Make passwords at least 8 characters long and use a mix of uppercase and lowercase letters, numbers, and symbols.
- Don't use your user name, real name, company name, or any complete words.
- Ensure new passwords are significantly different from previous ones.

Every 53 seconds, a laptop is stolen[5]

To safeguard your data and network:

- Keep your antivirus and operating system updated.
- Report stolen or malfunctioning devices to IT immediately.
- Enable security measures on every device and keep them close at hand or locked.

[1]Symantec, 2016 Internet Security Threat Report, June 2016 [2]PhishMe, Enterprise Phishing Susceptibility and Resiliency Report, 2016 [3]Stroz Friedberg as quoted by Microsoft, 2014
[4]Verizon Data, 2019 Data Breach Investigations Report, Security, 2017 [5]Gartner study commissioned by Kensington

How comprehensive safeguards from Microsoft can help

Here's how you can take advantage of built-in security features in Microsoft products to help keep your company safe.

Sender verification

Anti-spoofing technology in Microsoft 365 scans for forged "From" headers, which are the ones that show up in an email client like Outlook. When Microsoft technology can't authenticate a domain, it will mark those messages as spoofed, so you know not to click on them.

Data encryption

Encrypt sensitive emails and enable confidential protections with Microsoft 365 built-in security. Send encrypted and rights-protected messages to anyone inside or outside your organization—this protection will also extend to any attached Office 365 files.

Conditional access

Enroll your work devices according to company IT policy. Security policies get applied automatically to ensure proper encryption, strong passwords, virus protection, and current security updates.

Mobile safety

Your IT admin can remotely encrypt data with BitLocker or wipe sensitive data from a lost or stolen device with Microsoft 365 Device Management, so you can relax knowing your information is protected.

SYNNEX CORPORATION | Microsoft