



Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

DIGITAL SAFETY BASICS IN THE WORKPLACE

Renata Gutuzzo
2337141
Group 9
Digital Skills
LCLM4002



ENCRYPT ALL EMAIL ATTACHMENTS

Never send non-public information (NPI) in an unencrypted email attachment. You can easily encrypt email attachments using WinZip. NEVER store NPI in the body of an email.

**virtual
vaults**

STORE INFORMATION IN "VAULTS"

NEVER STORE NPI LOCALLY! If you must store NPI in Word, Docs, Sheets, Excel, etc., store them in Microsoft Vault or Google Vault. These tools enable you to store sensitive files in a 2FA secured, encrypted directory in the cloud.



ENABLE FULL DISK ENCRYPTION

Activate a feature that encrypts your entire hard drive when you're offline during the day, making it useless to intruders.



USE A VIRTUAL PRIVATE NETWORK (VPN)

VPNs use an encrypted connection over the Internet, ensuring that sensitive data is safely transmitted. It prevents intruders from eavesdropping on your internet traffic and effectively extends your agency's network far beyond its four walls.



USE TWO-FACTOR AUTHENTICATION

2FA technology requires two authentication methods to verify your identity: your password and a four to six-digit code texted to your smartphone. This second barrier makes it more difficult for someone to access your applications, emails, or devices.