



Navitas Global Student Privacy & Data Safety Guide



Why This Guide Matters

- Navitas collects your personal information to support your studies
- This guide explains how you can protect your personal data online
- It also provides information on what personal data is, and your Rights over how your personal data is used.
- Your use of Navitas IT systems is covered by the Student Acceptable Use Policy. This Policy is available via your student portal or college website
- You can contact us via privacy@navitas.com for any questions on personal data



In this Guide, You'll Learn About

- What personal data is
- Sensitive (special category) data
- Your privacy and rights as a student
- Scams and phishing
- Staying safe on public Wi-Fi
- Social medial and privacy
- Passwords and accounts
- How to get help



What is Personal Data?

PERSONAL DATA IS ANY INFORMATION THAT CAN IDENTIFY YOU.

COMMON STUDENT EXAMPLES

- Name & Contact Details
- Student ID Number
- Email Address
- Exam results
- Photos Or Class Recordings

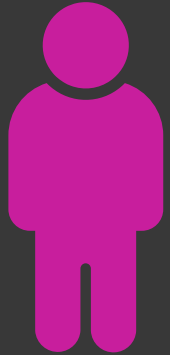
YOU MIGHT NOT REALISE THIS IS PERSONAL DATA

- Car Registration Number
- IP Address / Device Data
- CCTV Footage
- Bank Details

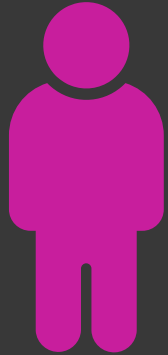
EVEN ONE DETAIL CAN BE PERSONAL DATA — ESPECIALLY WHEN COMBINED WITH OTHER INFORMATION.

Sensitive (Special Category Data)

SOME PERSONAL INFORMATION NEEDS EXTRA PROTECTION BECAUSE IT IS SENSITIVE.



Health, disability, or political beliefs



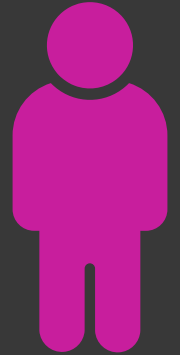
Race or ethnicity



Religion, philosophical beliefs, or Trade Union Membership



Sexual orientation, or criminal convictions and offences



Genetic or Biometric data

WHAT STUDENTS SHOULD DO?

Before sharing this type of information:



Make sure you understand why it's needed



Check how it will be used



Ask who it may be shared with

IF SOMETHING DOESN'T FEEL RIGHT, ASK QUESTIONS.

Your Privacy Rights

YOU HAVE RIGHTS OVER HOW YOUR PERSONAL INFORMATION IS USED. AS A STUDENT YOU CAN:



**ACCESS
YOUR PERSONAL
INFORMATION BY
REQUESTING A COPY**



**ASK FOR INCORRECT
OR INCOMPLETE
DETAILS TO BE
CORRECTED OR
COMPLETED**



**REQUEST DELETION OF
YOUR DATA**



**LIMIT OR
OBJECT
TO CERTAIN USES
OF YOUR DATA**



**ASK QUESTIONS
ABOUT HOW YOUR
DATA IS USED**

"HOW TO USE YOUR RIGHTS"

How to make a request:



Speak to your college, or



Email the Navitas Privacy Team at
privacy@navitas.com



Spotting Scams & Phishing

RECOGNISE SUSPICIOUS ACTIVITY THAT COULD PUT YOUR DATA AT RISK.



Unexpected emails
or messages
asking for your
details



Password reset
emails you didn't
request



Pop-ups asking
you to click links or
download files



New apps, files, or
changes you didn't
make

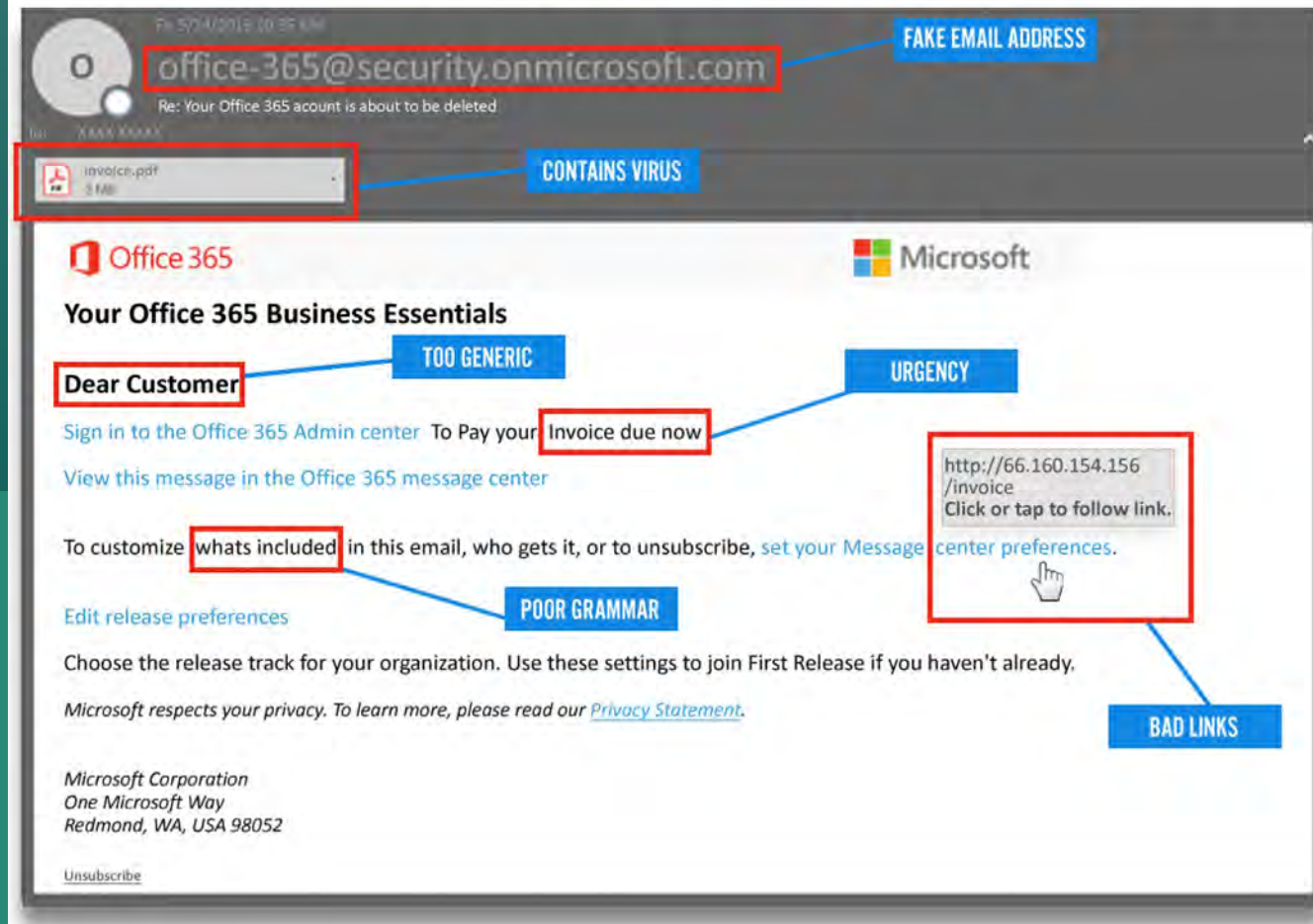


Unusual activity on
your accounts
(login attempts,
transactions)

IF IN DOUBT — DON'T CLICK, DON'T REPLY, AND REPORT IT TO YOUR COLLEGE OR EMAIL IT SUPPORT.

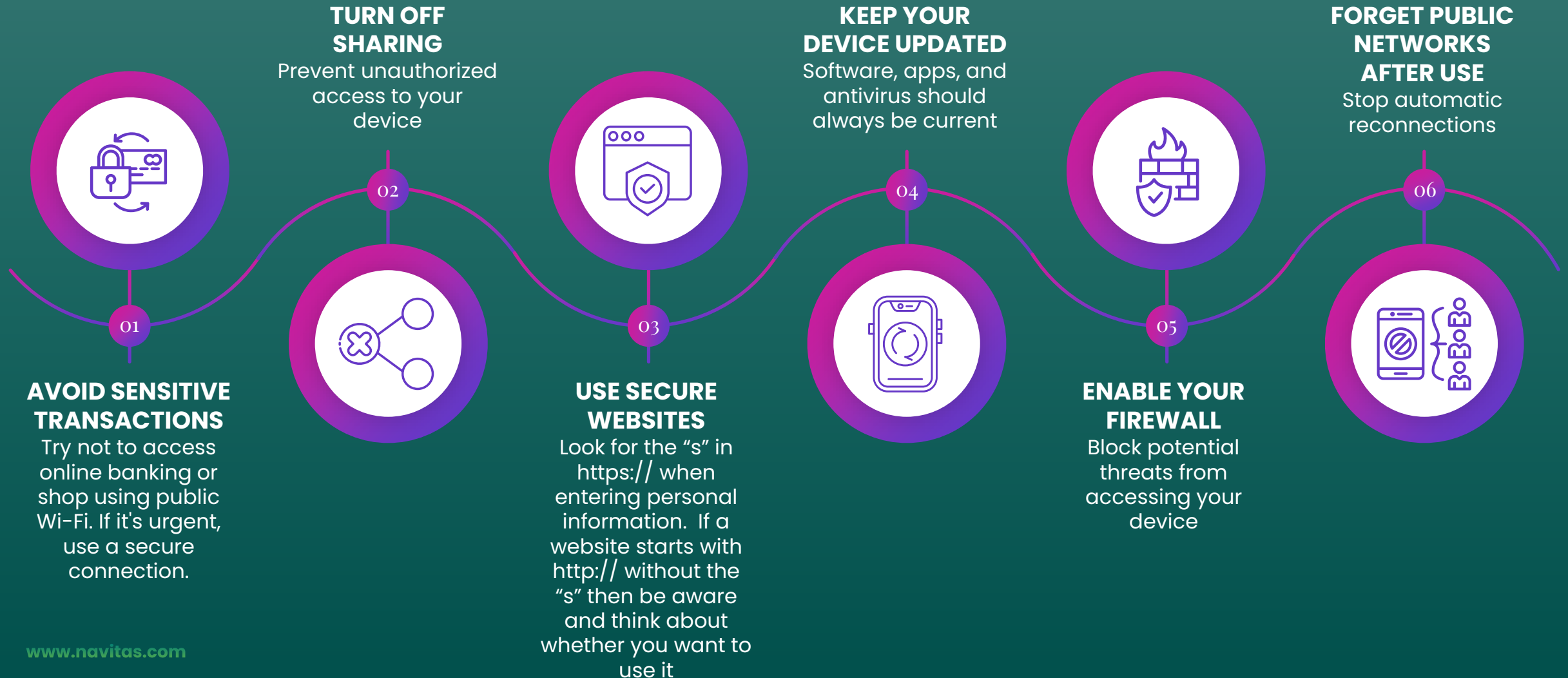
Recognising Fake Emails

Cyber criminals might send an email that looks legitimate, known as a phishing email, but you can take steps to avoid the traps



OFFICIAL COMMUNICATIONS WILL NEVER ASK FOR YOUR PASSWORD OR PERSONAL INFORMATION VIA EMAIL.

Staying Safe on Public Wi-Fi & Securing Personal Devices



Social Media & Your Privacy

WHAT YOU POST ONLINE CAN AFFECT YOUR PRIVACY.
HERE'S WHAT TO WATCH OUT FOR:



BE MINDFUL OF WHAT YOU SHARE

Avoid posting personal details like your address, ID numbers, or passwords



LIMIT YOUR AUDIENCE

Use privacy settings to control who can see your content



THINK BEFORE YOU POST

Once it's online, you may lose control over it



CHECK PLATFORM PRIVACY SETTINGS

Platforms e.g., Facebook, Instagram, TikTok, LinkedIn



READ PRIVACY NOTICES

As they explain how your data may be used



Passwords & Your Accounts

**YOUR ACCOUNT ACTIVITY IS YOUR RESPONSIBILITY.
KEEP YOUR PASSWORDS SAFE AND STRONG.**



Never share your password with anyone, even friends



Don't use anyone else's accounts—it puts their account and data at risk



Use strong, unique passwords — a mix of letters, numbers, and symbols works best



Use different passwords for different sites — don't reuse personal passwords



Change passwords if you suspect a breach

