Cyber Security

Communicating online safely & effectively.

Online etiquette at university.

Shane Reck
Cyber Security Analyst
Threat Actors – Who wants your info?

- **Recreational**
  - Fame and notoriety
  - Limited technical resources
  - Known exploits

- **Criminal**
  - Vandalism
  - Limited technical capabilities
  - Statement
  - Relentless, emotionally committed
  - Vast networks
  - Targeted attacks

- **Hacktivist**
  - Economic gain
  - Significant technical resources and capabilities
  - Established syndicates
  - Adware, crimeware, IP theft

- **Organized Crime**
  - State Sponsored
  - Cyberwar, state secrets, industrial espionage
  - Highly sophisticated
  - Nearly unlimited resources
  - Advanced persistent threats
Threat Breakdown

Crime and Fraud represents the largest overall cyber security threat.

Reports of cyber crime are increasing exponentially every year.

Why?
- Less physical risk to perpetrators compared to traditional crime.
- Easy to reach large numbers of victims.
- As technology improves so does a criminal’s opportunity to exploit it.
ALL your data has value

Stolen Fortnite accounts can sell for up to £200 depending on their content.

Thousands of email and social media account passwords are sold on the Dark web every day.

We detect 10-20 compromised student email accounts every week.

Imagine what your personal or research data is worth.
Be aware of what you share.

Email & Social Media:

• Don’t publish personal info such as Contact info, DOB, address or current location.

• Ensure your accounts are locked down (private).

• Don’t accept unsolicited requests/connections from people you don’t know.

• Consequences can include
  • Account theft
  • Personalised Phishing mails
  • Extortion
  • Identity theft
Digital Footprint

The record of your online activity. This may be recorded by several parties, including your ISP, employer and any website/service you interact with.

This record can affect your reputation and be leveraged by malicious persons.

**Active Footprint:**
- The emails you send
- Your shopping habits and product reviews
- Blogs you post or comment on
- Your social profiles and posts

**Passive Footprint:**
- IP Addresses
- Approximate Location
- Browsing history

Always assume your activity will be permanently recorded before you send, post or share.
Beware of Malicious Communications

Phishing is one of the most common types of cyber threat.

It is a form of Social Engineering:

Cyber Criminals will try to use your emotions against you, and exploit the natural human instinct to trust.

- Elation
- Urgency
- Fear
  - Negative consequences for non compliance.
  - Missing Out
Phishing - Social Engineering

Spam / Untargeted
- Generic messages sent in high volumes, targeting very low response rate.
- Often vague and poorly formatted.
- Highly prevalent due to availability of huge email lists on the dark web.

Spear phishing
- Tailored, targeted messages, often directly addressed to recipient.
- Sender will aim to give impression of authenticity using personal or not widely known information.

Spoofing
- Faking the display name or sender address of an influential person, or a person known to the recipient.
- Often used in conjunction with spear phishing.
- Easy to do and hard to detect.
Mitigation – How to Spot a Phish

Hover your mouse over links (long press on touch screens) to check where they will take you.
• Watch out for Imitation or “Look alike links”.

Verify the sender of any suspect emails.
• Search for contact info independently and contact them another way.
• Access the organisation’s website directly without clicking links or responding to the mail.

Be extremely wary of attachments
• Can contain malicious code.
• Always be sure the sender is valid before responding.
Not Just Email

Phishing can take several forms aside from Email:

- Vishing – Phishing via voice or video calls.
- SMiShing – Phishing via SMS, instant, or social media messaging.

Be aware of real world phishing too.
- Dumpster diving – shred your documents
- Shoulder Surfing – particularly in public places
- Tailgating
Money Muleing

A money mule is a person who transfers stolen money between different accounts, often to different countries.

Mules are recruited by criminals to receive money into their bank account, in order to withdraw and wire it overseas, receiving a commission payment in return.

More than 90% of money mule transactions are linked to cybercrime.

Source: Europol
Money Muleing

Mules are often recruited using fake job ads, social media ads, or direct contact via email.

Students and new arrivals to a country are both highly targeted groups.

If caught, money mules can face fines, community service, or prison sentences - Even if they were unaware they were committing a crime.

Beware offers of easy money.

If it seems too good to be true, it probably is.
Bottom Line

**Be Suspicious**, especially of unsolicited contact.

**Value your information.** Never share personal information or University Data with people you don’t know and trust. Consider your data just as valuable as your cash.

If you are being threatened or urged to take action quickly, someone may be trying to scam you.

Consider your online comms as a permanent record – **Be Nice**
Questions