Message analysis

Donation

Intention

- acquire personal information (to sell them or use them for something)

Red flags

- free money
- long emotional story
- asking for information
- many different email addresses to reply to
- undisclosed recipients (most likely a lot of them)

Prevention

- mark as spam, delete
- don't reply

Instagram

Intention

- login information

Red flags

- the user (most likely) hasn't changed their password, so email like this isn't expected -> suspicious
- sender domain name doesn't match instagram.com
- sense of urgency

Prevention

- see where the links point to (without opening them) to make sure it 100% isn't instagram
- spam, delete
- try to find out how they managed to associate IG account and email

Office 365

Intention

- login information
- compromising user in an organization

Red flags

- way too many `Sign in` buttons
- urgency -> employees can't work

Prevention

- notify superior/responsible people of potential spearphishing attempt
- mark spam
- don't click any links (not even the `unsubscribe` one)

MUNI

Intention

- login information
- link to malicious site

Red flags

- urgency
- automatically generated, translated
    - overall weird sentence structure
    - `Hi zahora`
    - `Requet` - not translated because of typo
- fake sender header
    - could be spearphishing?

Prevention

- notify MUNI sysadmins
- mark spam, delete

CV

Intention

- malware

Red flags

- simple mail with attachment
- attachment encrypted with password -> AV evasion
- classic word document with macro malware asking to enable macros
- either downloads malware from remote location, or extracts exe from document itself (commonly stored as tiny invisible base64 at the end)

Prevention

- (if working in a company, especially HR) notify superior/responsible people of potential spearphishing attempt

- spam, delete

Fedex

Intention

- login information
- personal information
- malicious website

Red flags

- `Hello mate` - official company but generic *pozdrav*
- sus link
  - nothing to do with fedex
  - doesn't even have package name in it smh
- "free package"

Prevention

- delete, ignore

Discord

Intention

- steal login info
- take over account, send the same message to other contacts

Red flags

- `dlscord-app.info`
  - `l` instead of `i`
  - not `discordapp.com` or `discord.com`
- free Nitro
- real Discord would most likely
  - remember users account and not ask for login
  - open and process link in app instead of web browser
- person spamming this to every channel they have access to -> bot

Prevention

- in server
  - ask mods to delete the message
  - warn dumb users that this is phishing
  - kick/ban user
  - alternatively you can use `Timeout user` feature until they get their account back

Blackmail

Intention

- get money

Red flags

- quite often they include recipients password acquired in data breach
- asking for money
- urgency -> 5 days to pay, sensitive content

Prevention

- mark spam, delete
- (if the data was real in the first place) even if you pay there would be no guarantee that you'd get what was promised
- if password at the start
  - check haveibeenpwned to see where the breach was from, and what other data was stolen
  - ^ either the websites hashing algorithm (if any) or your password is shit (possibly both)
  - make sure the same password is not used elsewhere

CIA

Intention

- get money

Red flags

- asking for money
- urgency -> you will be arrested

Prevention

- mark spam, delete

Steam

Intention

- steam login information

Red flags

- opens fake login window
  - can't be moved outside website area
  - has Windows 10 style even though user seems to be running Linux
  - has "Google Chrome" in name even though user is running Firefox
- login data is sent to `csgo500.org` directly

Prevention

- close website
- (stop gambling with CSGO skins)