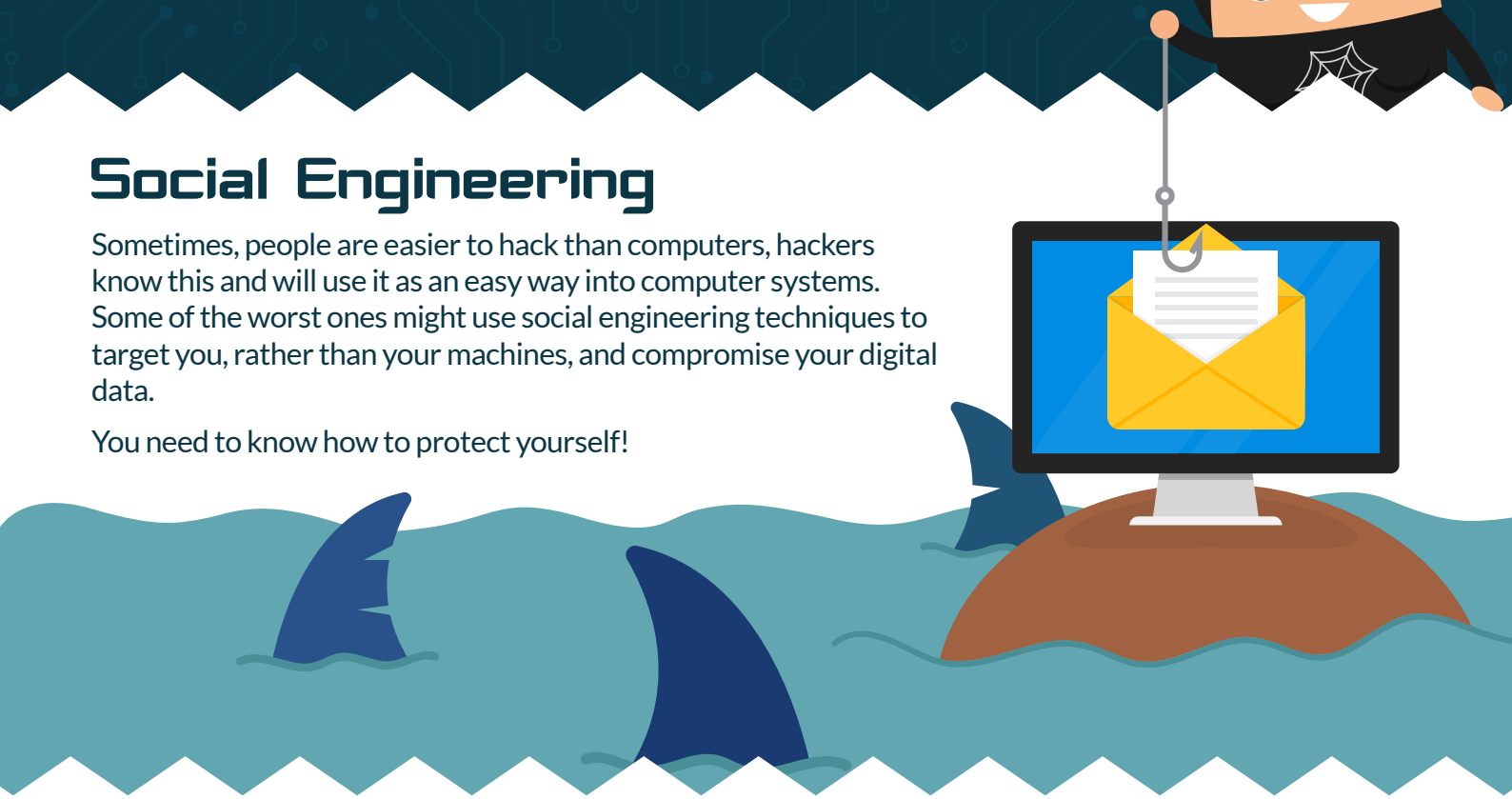
Preventing Attacks and Contingency

Social Engineering

Sometimes, people are easier to hack than computers, hackers know this and will use it as an easy way into computer systems. Some of the worst ones might use social engineering techniques to target you, rather than your machines, and compromise your digital data.

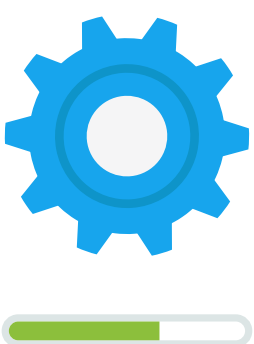
You need to know how to protect yourself!



Preventative tips:

Don't fall for obvious stuff.
So, things like phishing emails! Ignore pop-ups that masquerade themselves as official authorities. Like the FBI monitoring your 'illegal activity'. It's rubbish.

Don't ignore updates.
We know, they're annoying. But they're honestly there for a reason. Hackers sometimes get in through vulnerabilities in their systems, and doing your security updates can solve them.



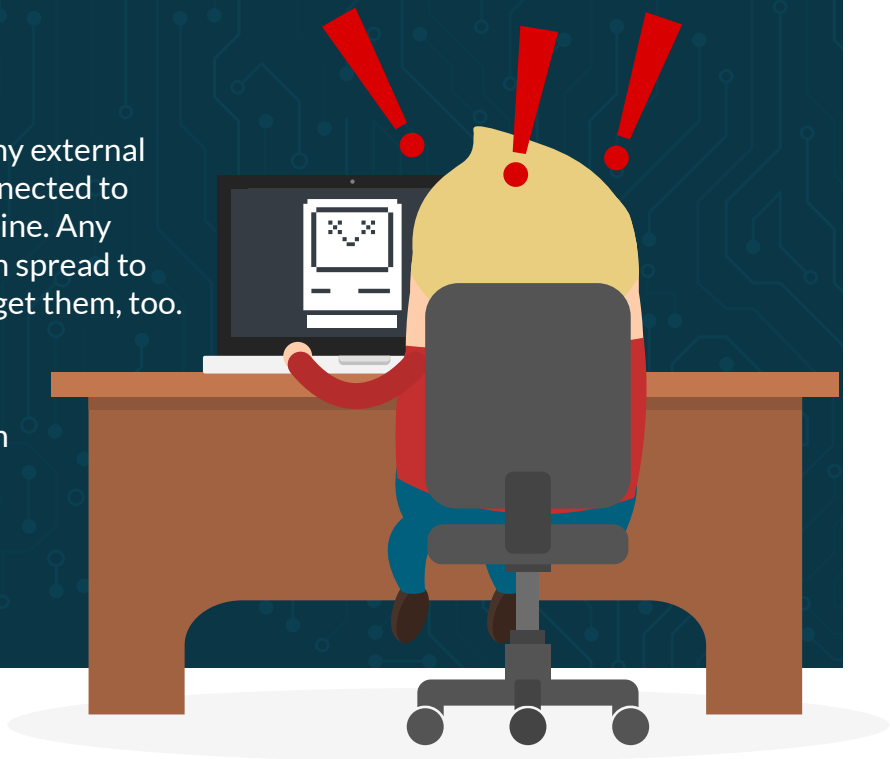
Back up.
Stop putting it off! All it takes is one nasty mistake and you could lose everything.

Disconnect.
Disconnect your hard drives and USBs when you're not using them. If your computer gets infected, those could get hit too.

Get Cybersecurity.
First off, find out if your computer needs it. If it does – look into some anti-malware software or a reputable security suite.

Contingency

1. Go offline. You can sometimes limit damage if you disconnect from your network right away.
2. Remove any external drives connected to your machine. Any viruses can spread to them and get them, too.
3. Size up the damage: work out which ransomware you've been affected with – this can help you deal with it.
4. Clean up your machine.



Report it!

We know what you're thinking. But contrary to what you might think – it's really important. So go ahead, be a grass.

Every report can help to give authorities a better idea on how these hackers operate.

We have to treat cybercrime like other crime.

Real-time reports of cybercrime, knowing what the criminals are up to, and gathering evidence will help do this!