PHISHING - WHAT IS IT?	**WHY SHOULD YOU CARE?**
Phishing is when a threat actor poses as a trusted source and sends fraudulent digital messages, such as emails, with the intent of manipulating individuals into revealing personal information and gaining unauthorized access to a system through a download or link.	Phishing attacks are some of the most commonly successful types of attacks. Learning how to recognize fraudulent messages by paying close attention to detail and never clicking on embedded hyperlinks, as well as remembering to report phishing attempts when you are targeted, are the best ways to defeat this kind of cyber attack. Ensure that URLs begin with "https:" when clicking on links. The "s" indicates encryption is enabled to protect users' information. Learn the signs of these types of attacks and think before you click. Check that emails and links are legitimate. Verify all attachments come from a trusted source.
MALWARE - WHAT IS IT?	**WHY SHOULD YOU CARE?**
Malware, short for "malicious software," is software intended to damage, disable or give someone unauthorized access to your computer or other internet-connected device. This includes adware, botnets, ransomware, rootkits, spyware, viruses, worms and numerous others.	Malware can disrupt networks, interrupt business operations or lead a person to malicious sites to scam them for money or harm their reputation.
RANSOMWARE - WHAT IS IT?	**WHY SHOULD YOU CARE?**
Ransomware is a type of malware in which the attacker encrypts the victim's data to make it as inaccessible as possible, often by locking a person completely out of their computer. The hacker then demands a ransom to release or unencrypt that information.	The fees extorted by ransomware can be extreme or prohibitive — not to mention that there is no guarantee that your data will be returned after a ransom is paid! In addition to keeping your software and antivirus programs up to date, regularly back up your system on the cloud or on an external hard drive. That way, you always have a spare copy of the information that is most important to you or your business.
BOTS - WHAT ARE THEY?	**WHY SHOULD YOU CARE?**
Bots can carry out useful functions or be invasive and harmful. Bots are automated with pre-defined tasks that can imitate or replace human user behavior.	Bots can come as malware and gain total control over a computer system. They can scan or obtain contact information, send spam or perform other harmful acts.
SOCIAL ENGINEERING - WHAT IS IT?	**WHY SHOULD YOU CARE?**
Sometimes threat actors do not need computers to gain access to your information. With social engineering, threat actors gather common information about you to trick you into giving unauthorized access to information systems. Social engineering attacks can be quite sophisticated and are not always easy to recognize. This includes attacks such as phishing, swatting and more.	Social engineering attacks do not require sophisticated programming skills to be successful. The information you post on social media and other sharing platforms may make you especially vulnerable to these attacks.

PROTECT YOURSELF ONLINE

There are four easy ways to protect yourself online:

1. **Enable multi-factor authentication (MFA)**
2. **Use strong passwords**
3. **Recognize and report phishing**
4. **Update your software**

OTHER AVENUES OF ATTACK

Any device that stores information or is connected to the internet can be a way for cyber criminals to gain access to your information systems – or, in some cases, use your devices to attack someone else. Assume that you are vulnerable and take measures to understand and mitigate risk.

PASSWORD TIPS

One of the first lines of defense for keeping your information safe online is the use of a password. Some password tips are as follows:

- **Use different passwords on different accounts.** One of the leading causes of unauthorized access to accounts is the reuse of login credentials (*see* National Cyber Awareness System Tips—Choosing and Protecting Passwords).
- **Use the longest password allowed.** The longer and more complicated a password is, the harder it will be for someone to access your accounts. Use 11 characters or more, a short sentence or a mix of letters, symbols and numbers to strengthen your passwords.
- **Reset your password every few months.** Reset your passwords regularly, especially when these passwords allow access to confidential accounts, such as banking or medical data. It is vital to reset passwords as it takes most companies an average of six months to notice that a data breach has happened. By the time a data breach is reported, a threat actor could already be using and/or selling your data.
- **Use a password manager.** With just one master password, a password manager can generate and retrieve passwords for every account that you have – encrypting and protecting your online information, including credit card numbers and their three-digit Card Verification Value (CVV) codes, answers to security questions and more.

National Cyber Security Centre

10 Steps to Cyber Security

Defining and communicating your Board's Information Risk Regime is central to your organisation's overall cyber security strategy. The National Cyber Security Centre recommends you review this regime – together with the nine associated security areas described below, in order to protect your business against the majority of cyber attacks.

Network Security

Protect your networks from attack. Defend the network perimeter, filter out unauthorised access and malicious content. Monitor and test security controls.

User education and awareness

Produce user security policies covering acceptable and secure use of your systems. Include in staff training. Maintain awareness of cyber risks.

Malware prevention

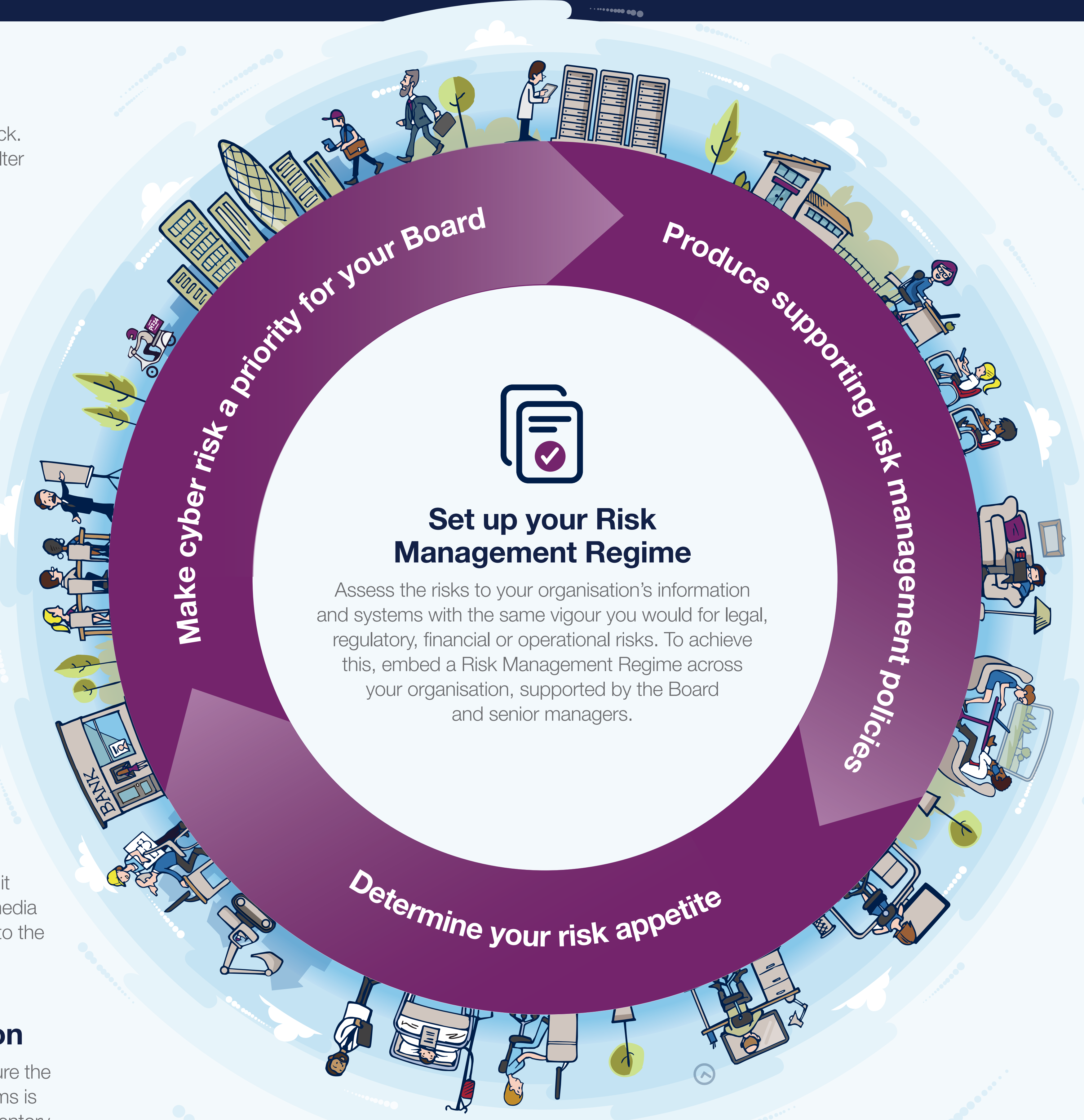
Produce relevant policies and establish anti-malware defences across your organisation.

Removable media controls

Produce a policy to control all access to removable media. Limit media types and use. Scan all media for malware before importing onto the corporate system.

Secure configuration

Apply security patches and ensure the secure configuration of all systems is maintained. Create a system inventory and define a baseline build for all devices.



Make cyber risk a priority for your Board

Produce supporting risk management policies

Determine your risk appetite

Set up your Risk Management Regime

Assess the risks to your organisation's information and systems with the same vigour you would for legal, regulatory, financial or operational risks. To achieve this, embed a Risk Management Regime across your organisation, supported by the Board and senior managers.

Managing user privileges

Establish effective management processes and limit the number of privileged accounts. Limit user privileges and monitor user activity. Control access to activity and audit logs.

Incident management

Establish an incident response and disaster recovery capability. Test your incident management plans. Provide specialist training. Report criminal incidents to law enforcement.

Monitoring

Establish a monitoring strategy and produce supporting policies. Continuously monitor all systems and networks. Analyse logs for unusual activity that could indicate an attack.

Home and mobile working

Develop a mobile working policy and train staff to adhere to it. Apply the secure baseline and build to all devices. Protect data both in transit and at rest.

For more information go to 🖥 www.ncsc.gov.uk @ncsc