

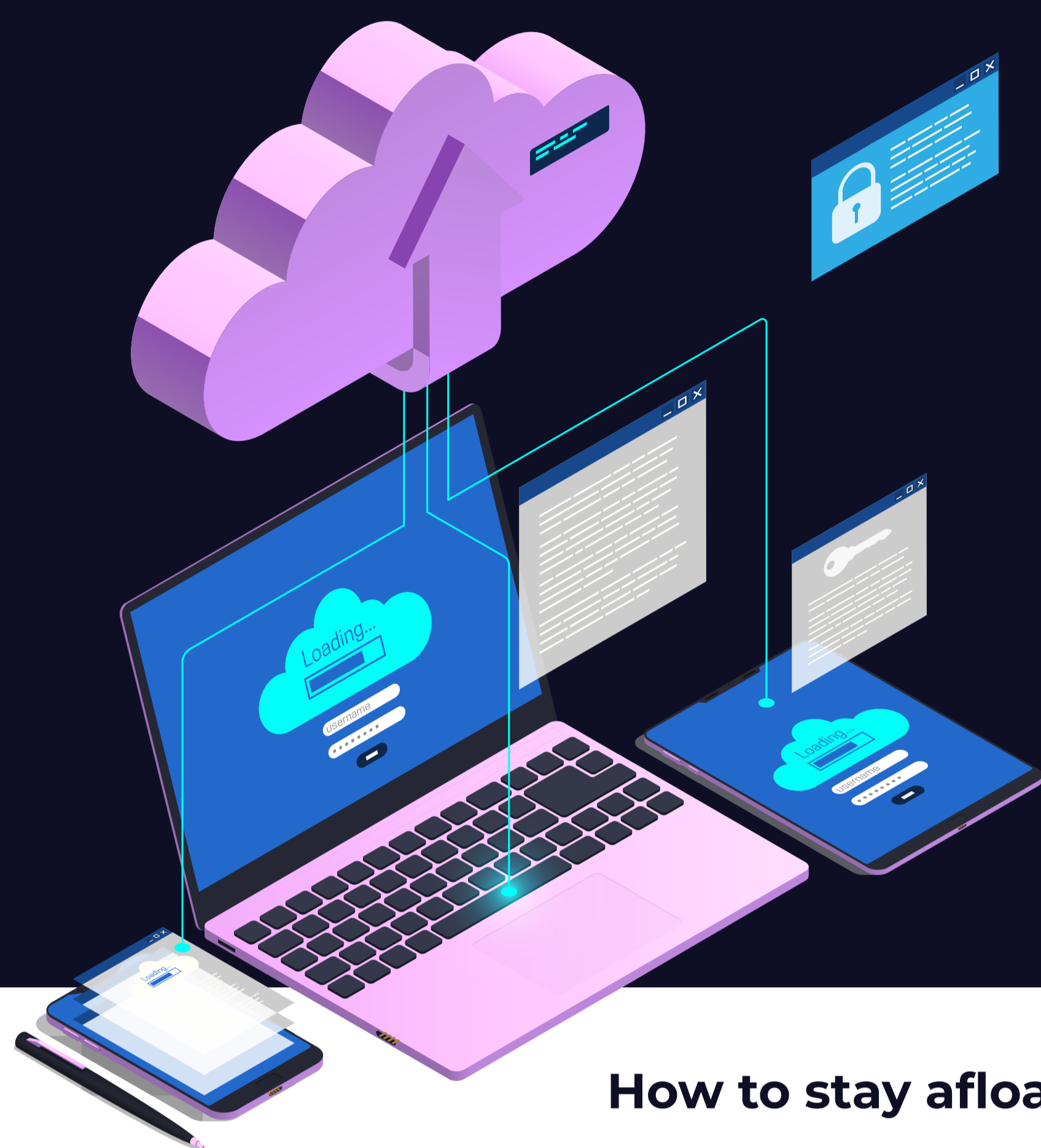
Cybersecurity

Cybersecurity Basics:

The lifejacket you need while surfing the web

Cybersecurity is an art form that addresses the protection of information in the digital age. Your personal information is stored on your laptop, smartphone, or tablet. It's important to know how to protect your information from cyber criminals. Every time you use the internet, you face choices related to your cybersecurity.

HERE ARE SOME TIPS TO PROTECT YOU AGAINST HARMFUL ONLINE ATTACKS:



1. Think Before You Click:

Cybercriminals are masters of disguise; they make use of "phishing" to pretend to be someone or something else. They use email, text, or malicious websites to infect your digital devices with malware. They attempt to lure users to click on a link or open an attachment that infects their computers or mobile phone and makes the user vulnerable to an attack.

Have a look at this example:

"Our records indicate that your account was overcharged. You must call us within 7 days to receive your refund." – This message creates a sense of urgency for the user and lures them in with a financial scare tactic.



How to stay afloat while surfing the web:

- Don't fall for a cybercriminal's trick.**
 Even if you get an email, text or post that looks legit, it might not be. If it's not from someone you know, or if it contains links, be suspicious—and don't click on anything. If you think the message might be real call the company or person directly to make sure.
- Beware of the hyperlink.**
 Don't click on anything unfamiliar, and hover over links to verify their authenticity. Make sure URLs start with "https"—the "s" indicates encryption is enabled to protect your information.

- Once you post on the internet, it's out there forever.**
 Keep personal information to yourself; don't give away vital details about your job title, full name, birth date and more if you don't have to. If people know the vital details about your life, they can attempt a direct "spear-phishing" attack on you by trying to coax you into giving up more information.

2. Update Your Software:

Don't put off software updates! They're not just for your phone—you should update your computer too.

As you know, cybercrime is a dangerous thing. It can steal your identity and destroy your data. To protect yourself from falling victim to this kind of crime, it's important to use anti-virus software, keep it up-to-date, and make sure that automatic updates are enabled on your computer.

Antivirus software examples:

- Bitdefender
- Trend Micro
- SentinelOne EDR (next-gen Antivirus)

4. Enable Multi-Factor Authentication:

The media is always reporting on security breaches, stolen data, and identity theft. Perhaps you or someone you know are victims of cyber criminals. Don't become a statistic—use multi-factor authentication (MFA), also called strong authentication, or two-factor authentication.

How and when MFA should be used:

You can describe someone's credentials as either "something you know," "something you have," or "something you are." Here's an example of each:

- Something You Know: Password/passphrase, PIN.
- Something You Have: Security token or software application, verification text, call, email, or smart card.
- Something You Are: Fingerprint, facial recognition, voice recognition.

Adding MFA to your logins is a great way to make sure only you can get into your account. It's like getting a second password but from your phone or email instead of your brain.

3. Use Strong Passwords:

The best way to keep yourself safe online is to use a long, random, and unique password but the most secure way to store all your unique passwords is by using a password manager.

Password Tips:

- Use a long, complex passphrase with 12 or more characters.**
 If you're using a password manager, make sure to use the longest possible password or passphrase allowed by it. For instance, you could use a quote from your favourite book as a password, or even the title of your favourite book.
- If a website asks you to choose a password, make it something difficult to guess.**
 No personal information, like your name or pet's name. These things are too easy to find on social media, which makes it easier for cybercriminals to hack your accounts.
- Passwords should be a secret**
 Don't tell anyone your passwords and watch out for attackers trying to trick you into revealing your passwords through email or by phone. Every time you share or reuse a password, it chips away at your security by opening more ways with which it could be misused or stolen.
- Use a different password for every account**
 To prevent cybercriminals from gaining access to your accounts and protect you in the event of a breach.

Follow the above tips and put on your lifejacket.

The Internet can be a vast and tumultuous sea, but if you stay afloat by following our advice, you'll avoid the sharks!