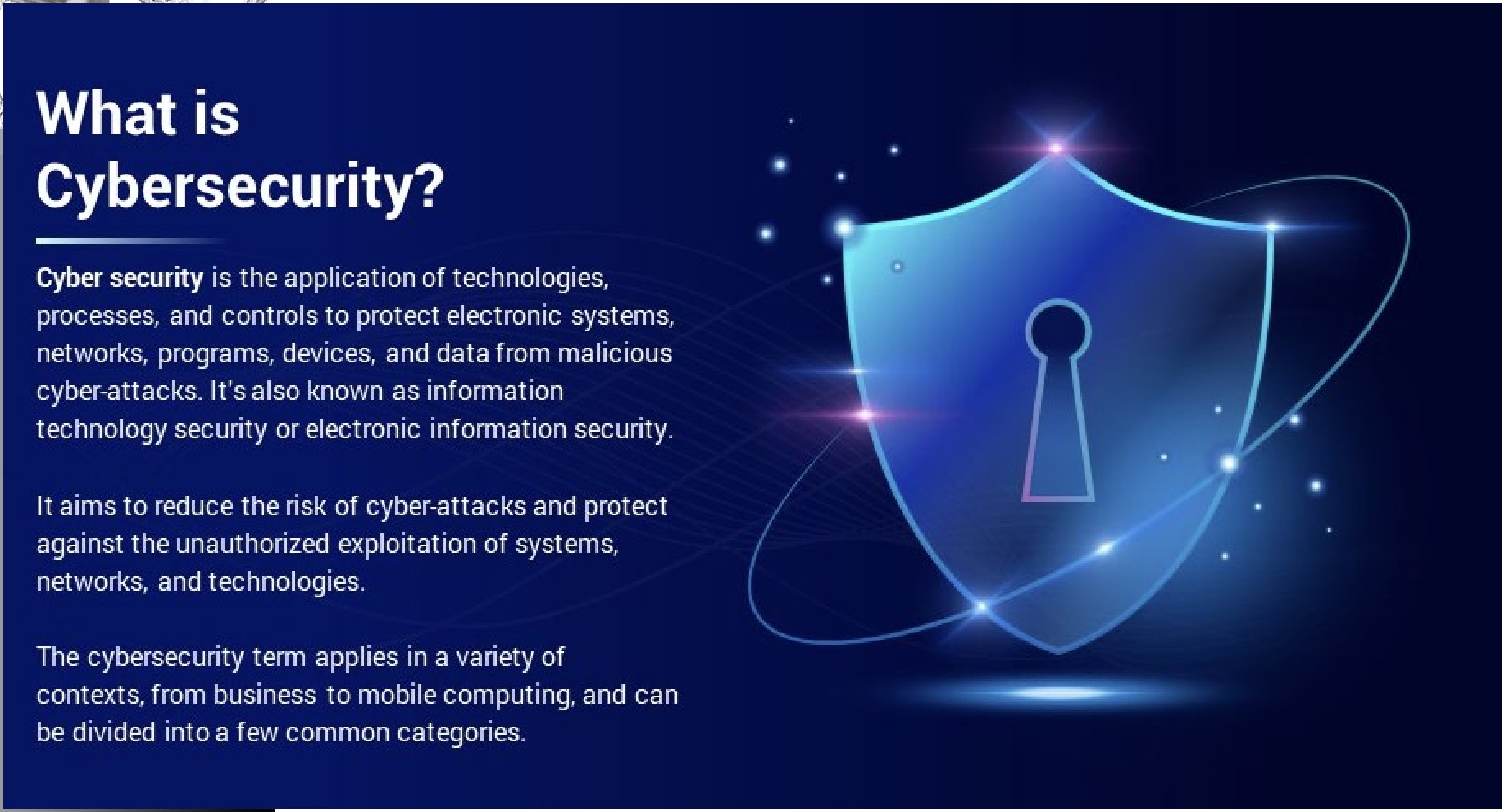
IMAGINE ROTARY

Rotary District 9810

DISTRICT 9810

Online Cybersecurity & avoiding scams

What is Cybersecurity?



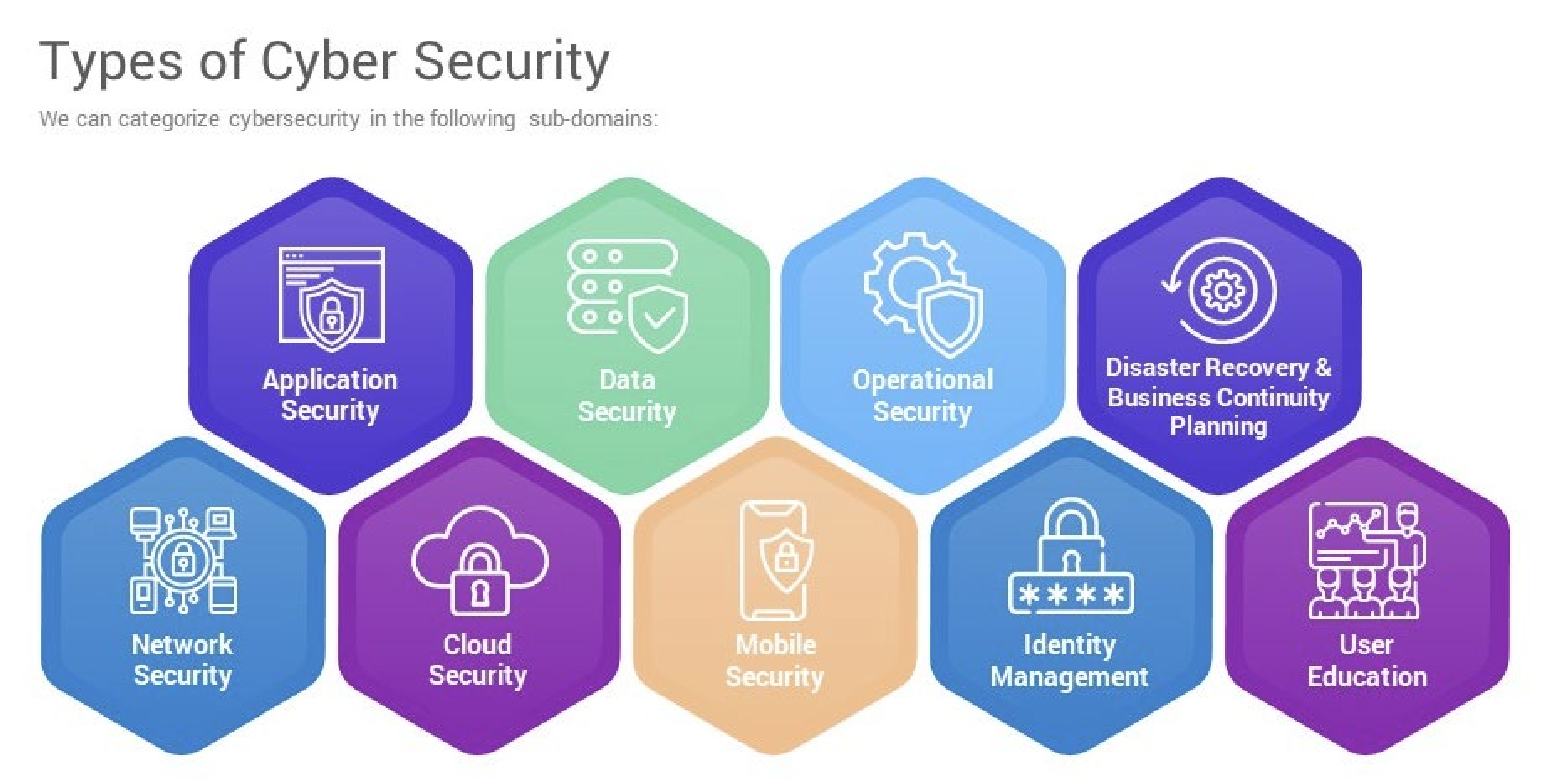
What is Cybersecurity?

Cyber security is the application of technologies, processes, and controls to protect electronic systems, networks, programs, devices, and data from malicious cyber-attacks. It's also known as information technology security or electronic information security.

It aims to reduce the risk of cyber-attacks and protect against the unauthorized exploitation of systems, networks, and technologies.

The cybersecurity term applies in a variety of contexts, from business to mobile computing, and can be divided into a few common categories.

Types of Cybersecurity

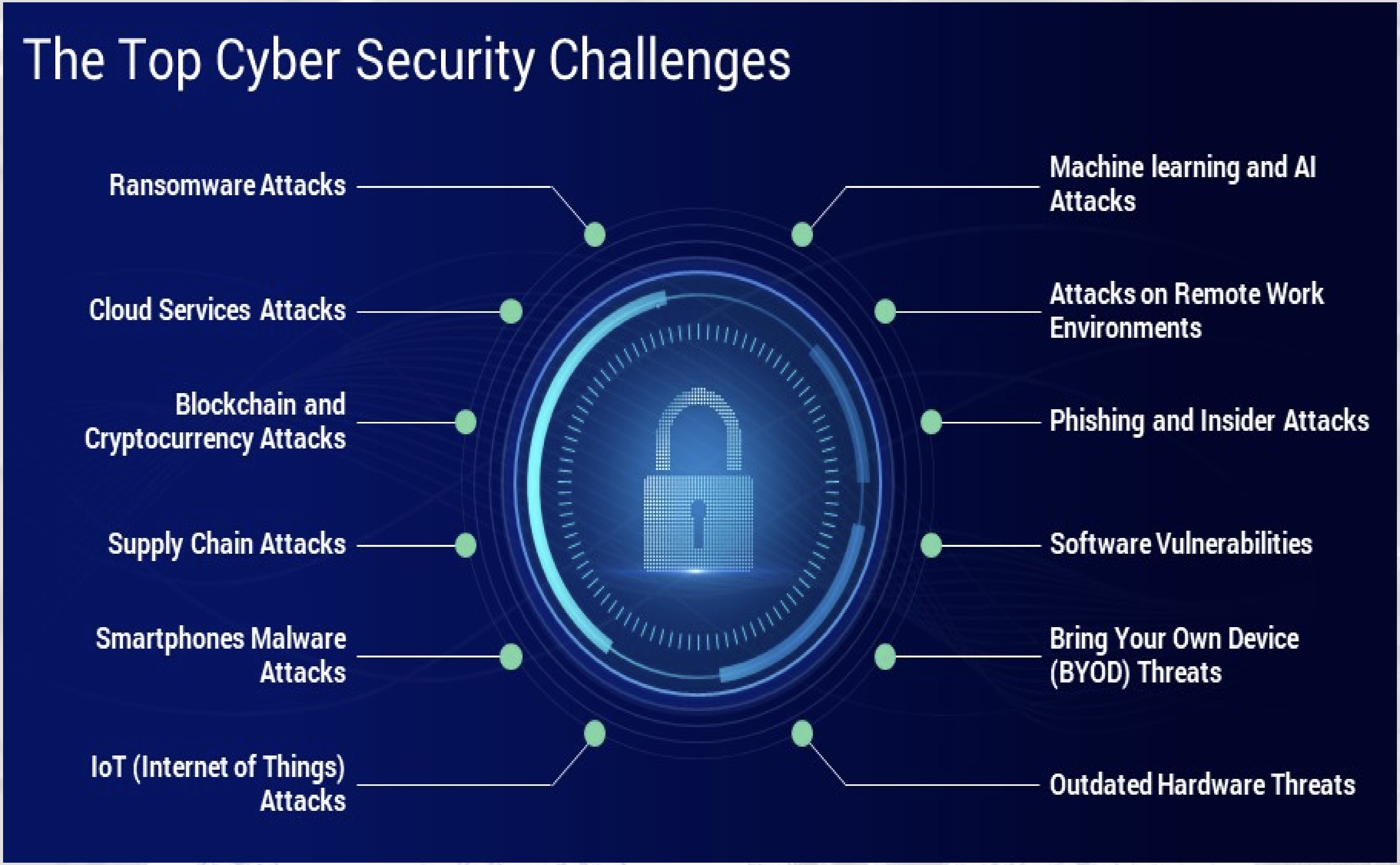


Types of Cyber Security

We can categorize cybersecurity in the following sub-domains:

- Application Security
- Data Security
- Operational Security
- Disaster Recovery & Business Continuity Planning
- Network Security
- Cloud Security
- Mobile Security
- Identity Management
- User Education

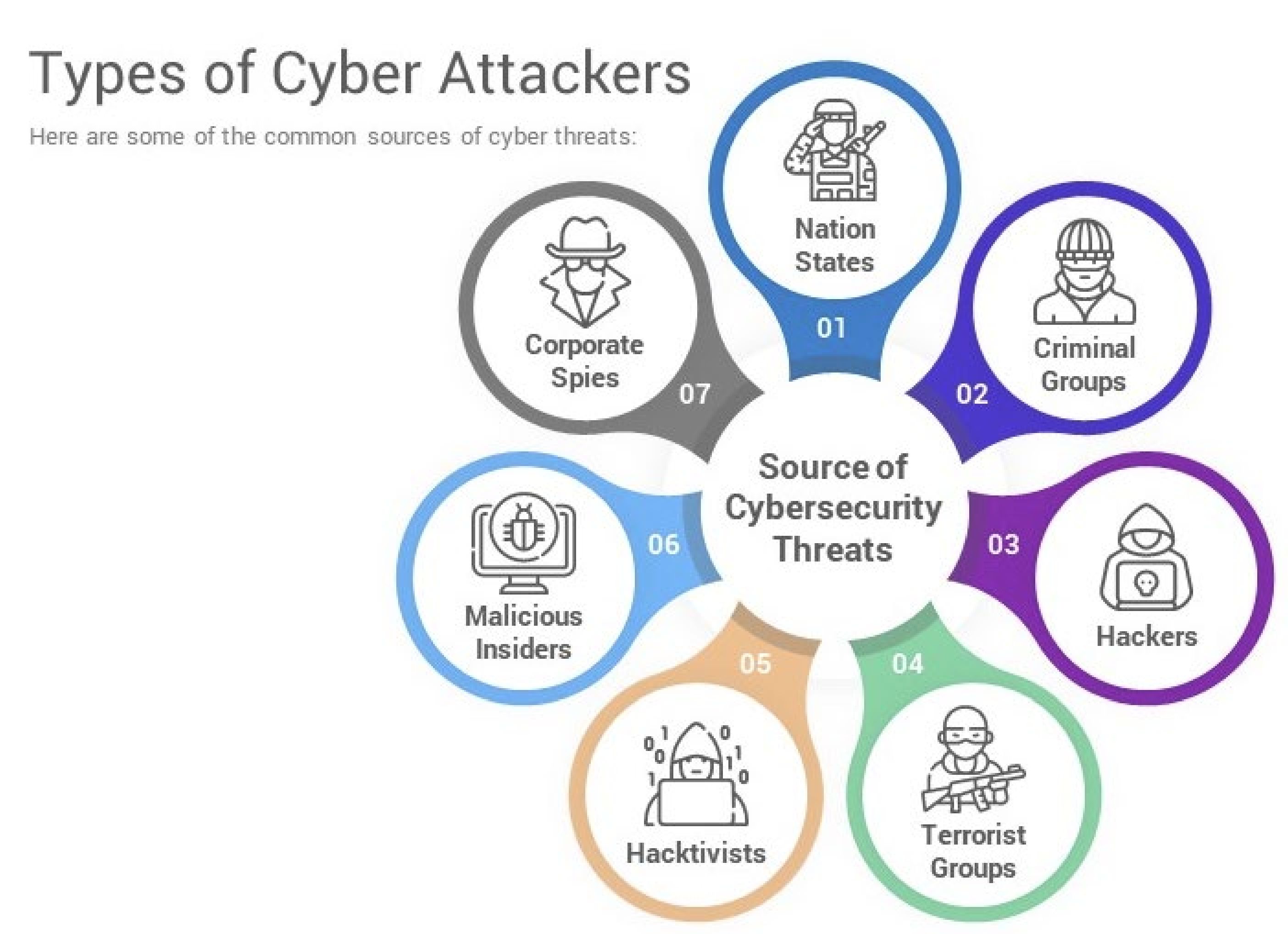
Top Cyber Security Challenges



The Top Cyber Security Challenges

- Ransomware Attacks
- Cloud Services Attacks
- Blockchain and Cryptocurrency Attacks
- Supply Chain Attacks
- Smartphones Malware Attacks
- IoT (Internet of Things) Attacks
- Machine learning and AI Attacks
- Attacks on Remote Work Environments
- Phishing and Insider Attacks
- Software Vulnerabilities
- Bring Your Own Device (BYOD) Threats
- Outdated Hardware Threats

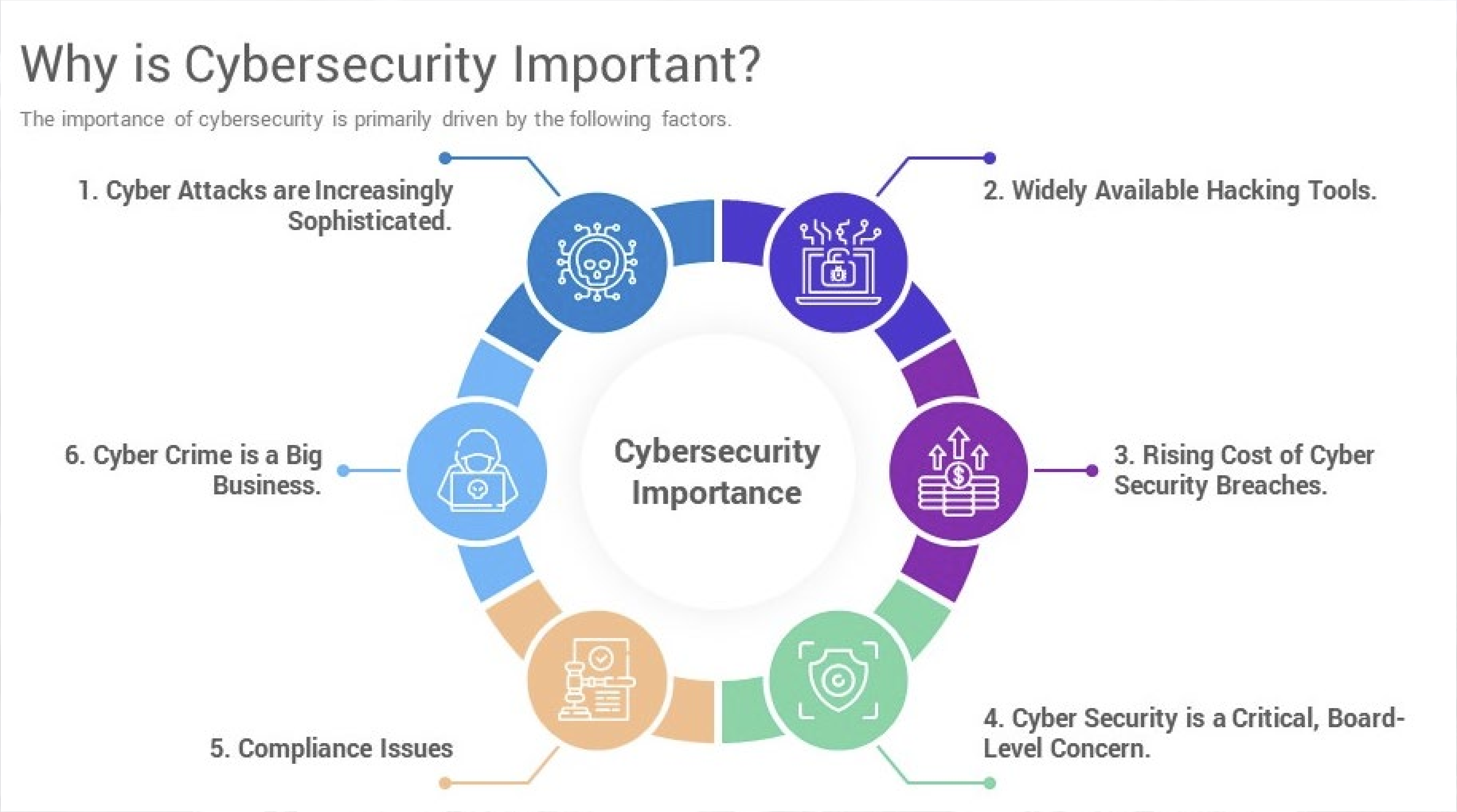
Types of Cyber Attackers



Types of Cyber Attackers

Here are some of the common sources of cyber threats:

Why is Cybersecurity Important?



Why is Cybersecurity Important?

The importance of cybersecurity is primarily driven by the following factors.

1. Cyber Attacks are Increasingly Sophisticated.

2. Widely Available Hacking Tools.

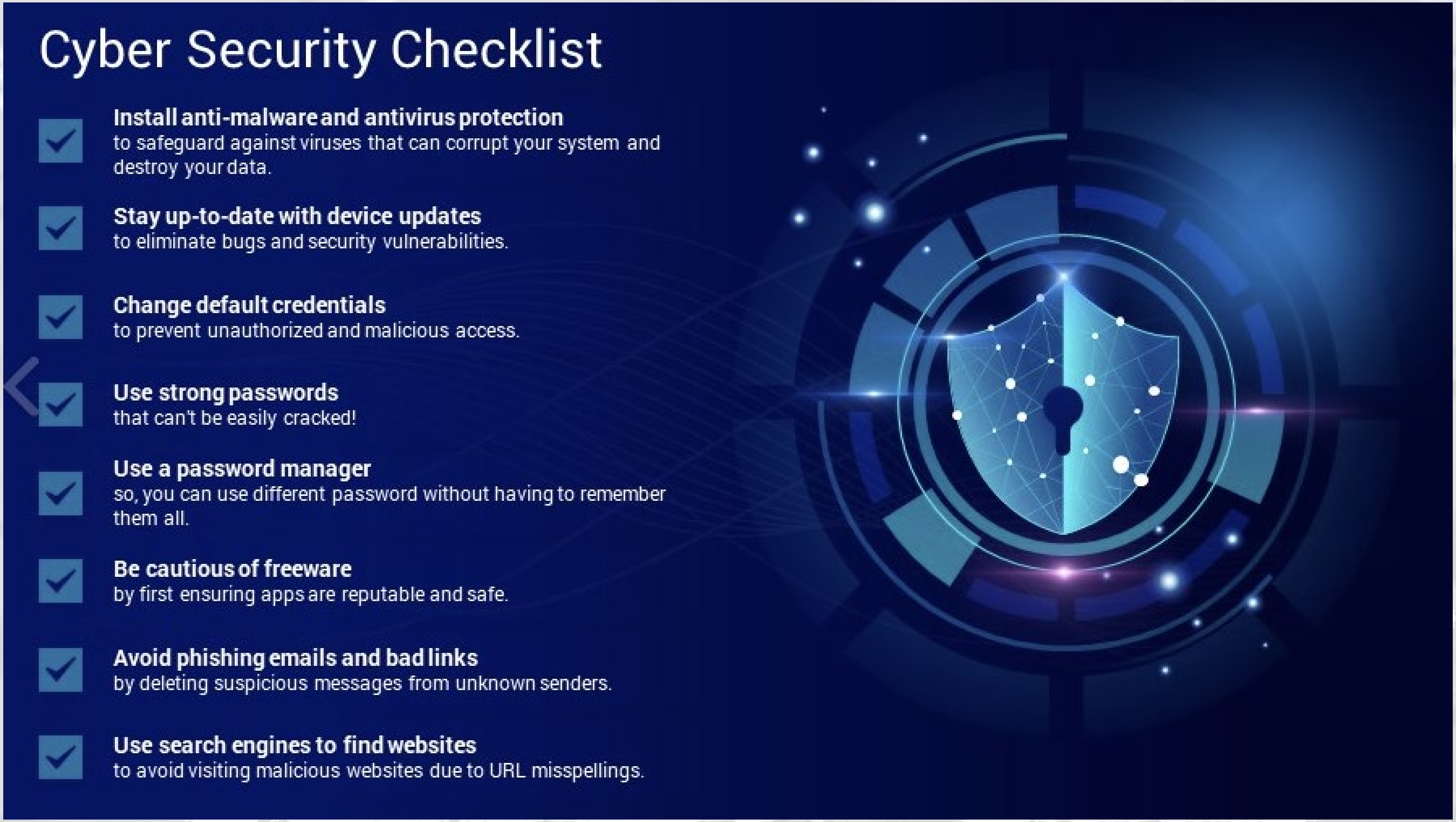
3. Rising Cost of Cyber Security Breaches.

4. Cyber Security is a Critical, Board-Level Concern.

5. Compliance Issues

6. Cyber Crime is a Big Business.

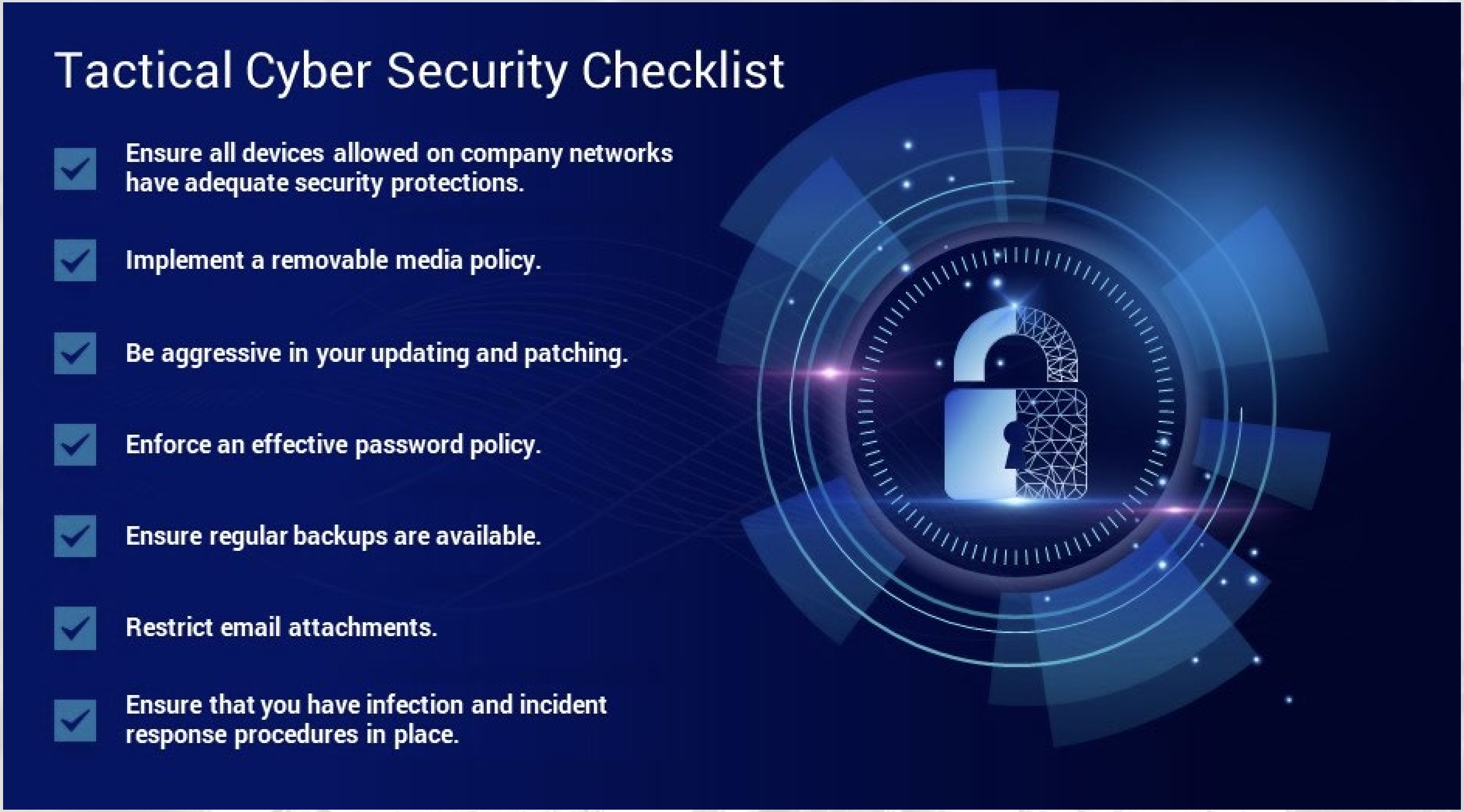
Tactical Cyber Security Checklist



Cyber Security Checklist

- ☑ **Install anti-malware and antivirus protection** to safeguard against viruses that can corrupt your system and destroy your data.
- ☑ **Stay up-to-date with device updates** to eliminate bugs and security vulnerabilities.
- ☑ **Change default credentials** to prevent unauthorized and malicious access.
- ☑ **Use strong passwords** that can't be easily cracked!
- ☑ **Use a password manager** so, you can use different password without having to remember them all.
- ☑ **Be cautious of freeware** by first ensuring apps are reputable and safe.
- ☑ **Avoid phishing emails and bad links** by deleting suspicious messages from unknown senders.
- ☑ **Use search engines to find websites** to avoid visiting malicious websites due to URL misspellings.

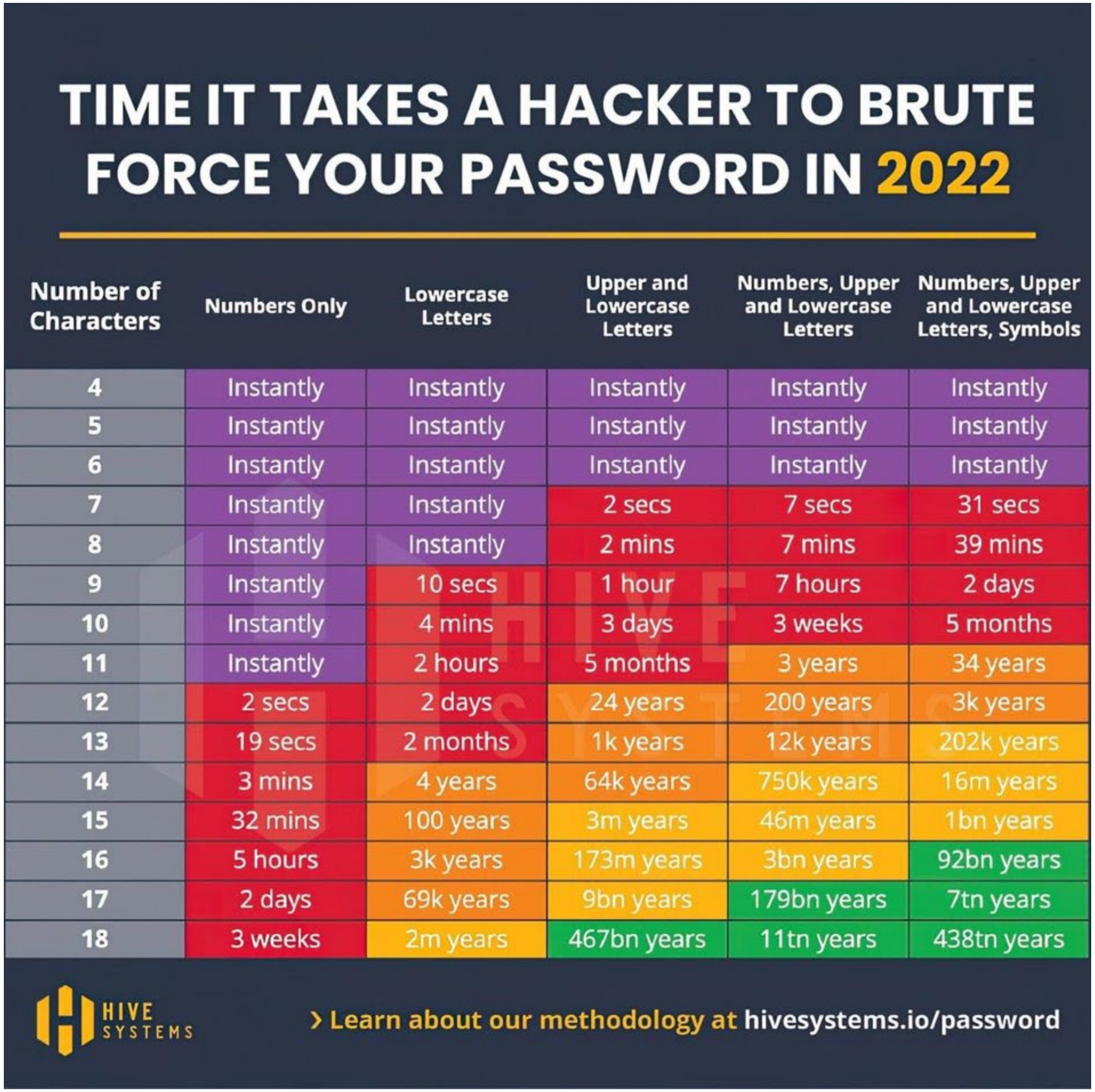
Tactical Cyber Security Checklist



Tactical Cyber Security Checklist

- ☑ Ensure all devices allowed on company networks have adequate security protections.
- ☑ Implement a removable media policy.
- ☑ Be aggressive in your updating and patching.
- ☑ Enforce an effective password policy.
- ☑ Ensure regular backups are available.
- ☑ Restrict email attachments.
- ☑ Ensure that you have infection and incident response procedures in place.

Secure passwords….



TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD IN 2022

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	2 secs	7 secs	31 secs
8	Instantly	Instantly	2 mins	7 mins	39 mins
9	Instantly	10 secs	1 hour	7 hours	2 days
10	Instantly	4 mins	3 days	3 weeks	5 months
11	Instantly	2 hours	5 months	3 years	34 years
12	2 secs	2 days	24 years	200 years	3k years
13	19 secs	2 months	1k years	12k years	202k years
14	3 mins	4 years	64k years	750k years	16m years
15	32 mins	100 years	3m years	46m years	1bn years
16	5 hours	3k years	173m years	3bn years	92bn years
17	2 days	69k years	9bn years	179bn years	7tn years
18	3 weeks	2m years	467bn years	11tn years	438tn years

HIVE SYSTEMS

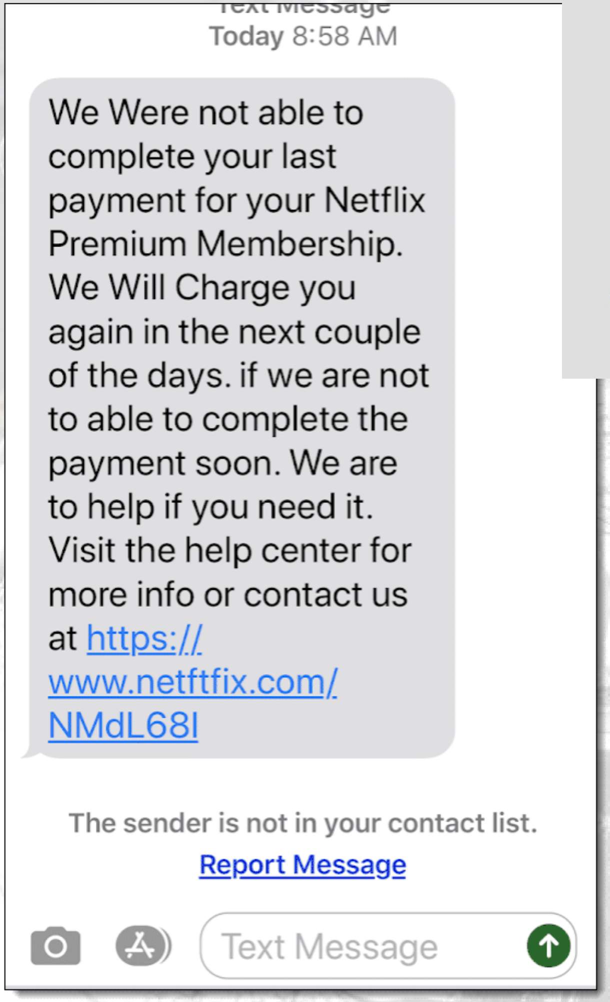
› Learn about our methodology at hivesystems.io/password

Most common

- Tax Scam
- Tech Support scam
- Finance Scam
- Identity Scam
- Parcel scam

How

- Phone Scams
- Text Messages
- Emails

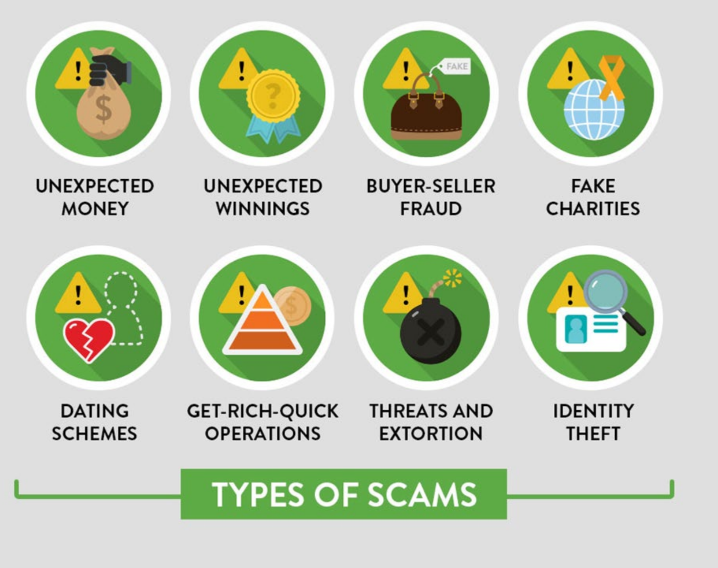


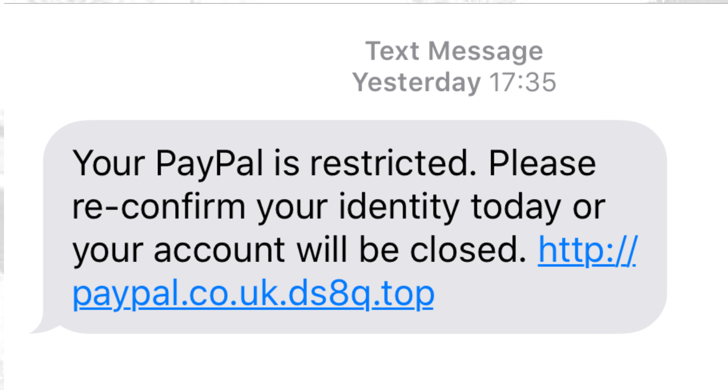
Text Message
Today 8:58 AM

We Were not able to complete your last payment for your Netflix Premium Membership. We Will Charge you again in the next couple of the days. if we are not to able to complete the payment soon. We are to help if you need it. Visit the help center for more info or contact us at https://www.netftfix.com/NMdL68I

The sender is not in your contact list.
Report Message

Text Message



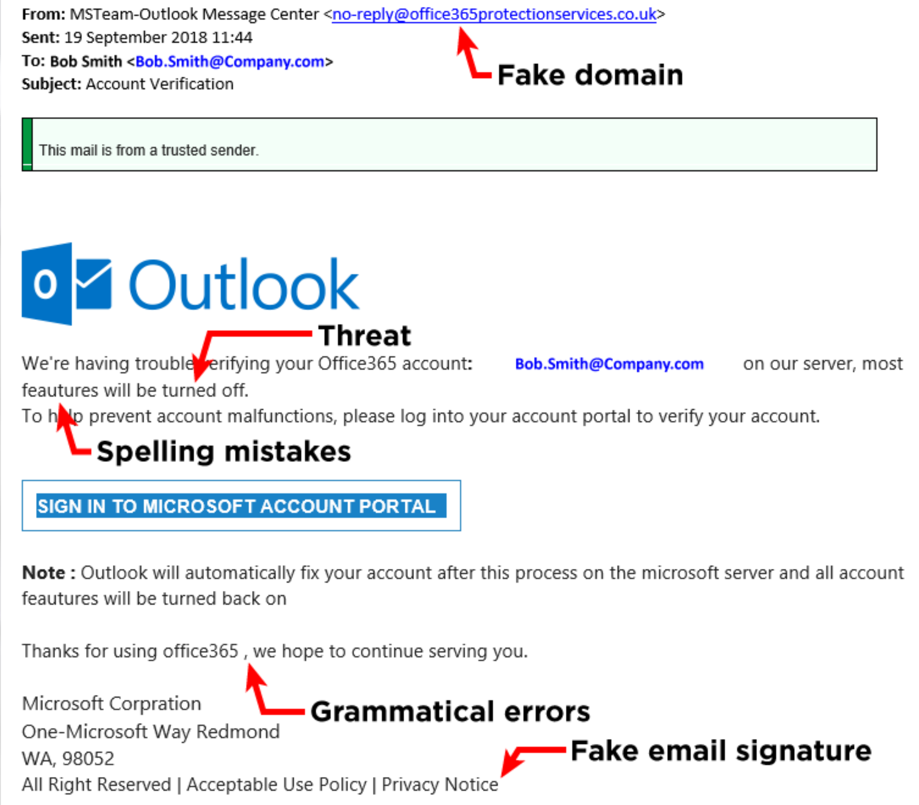


Text Message
Yesterday 17:35

Your PayPal is restricted. Please re-confirm your identity today or your account will be closed. http://paypal.co.uk.ds8q.top

What do I look for…….

- Check email extensions
- Check spelling & grammatical errors



From: MSTeam-Outlook Message Center <no-reply@office365protectionservices.co.uk>
Sent: 19 September 2018 11:44
To: Bob Smith <Bob.Smith@Company.com>
Subject: Account Verification

This mail is from a trusted sender.

Outlook

We're having trouble verifying your Office365 account: Bob.Smith@Company.com on our server, most feautures will be turned off.
To help prevent account malfunctions, please log into your account portal to verify your account.

SIGN IN TO MICROSOFT ACCOUNT PORTAL

Note : Outlook will automatically fix your account after this process on the microsoft server and all account feautures will be turned back on

Thanks for using office365 , we hope to continue serving you.

Microsoft Corpration
One-Microsoft Way Redmond
WA, 98052
All Right Reserved | Acceptable Use Policy | Privacy Notice

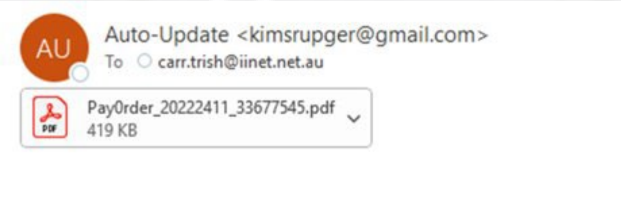
Fake domain

Threat

Spelling mistakes

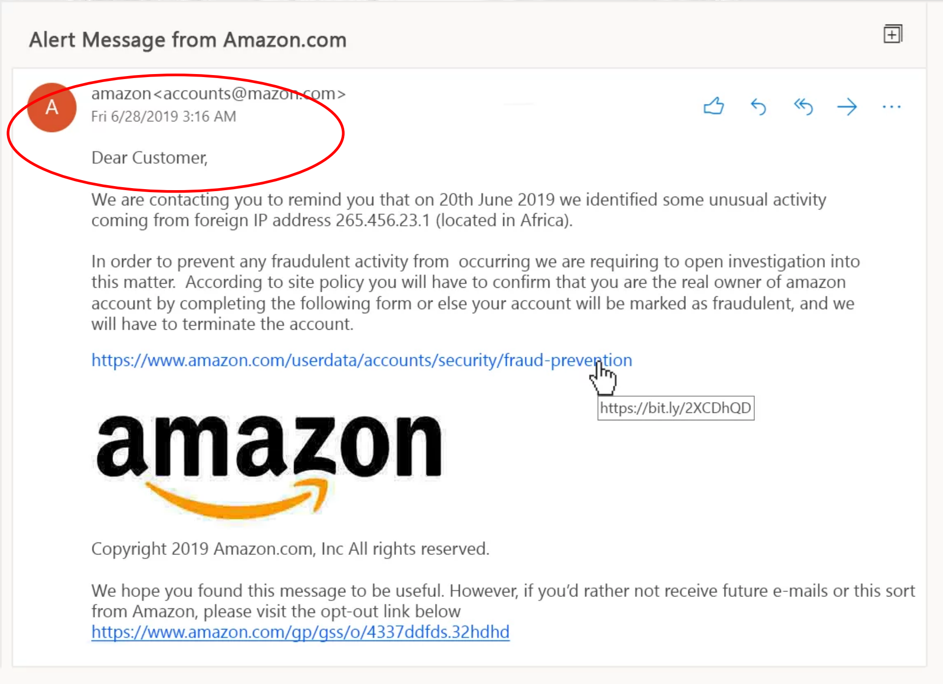
Grammatical errors

Fake email signature



Auto-Update <kimsrupger@gmail.com>
To ○ carr.trish@iinet.net.au

PayOrder_20222411_33677545.pdf
419 KB



Alert Message from Amazon.com

amazon<accounts@mazon.com>
Fri 6/28/2019 3:16 AM

Dear Customer,

We are contacting you to remind you that on 20th June 2019 we identified some unusual activity coming from foreign IP address 265.456.23.1 (located in Africa).

In order to prevent any fraudulent activity from occurring we are requiring to open investigation into this matter. According to site policy you will have to confirm that you are the real owner of amazon account by completing the following form or else your account will be marked as fraudulent, and we will have to terminate the account.

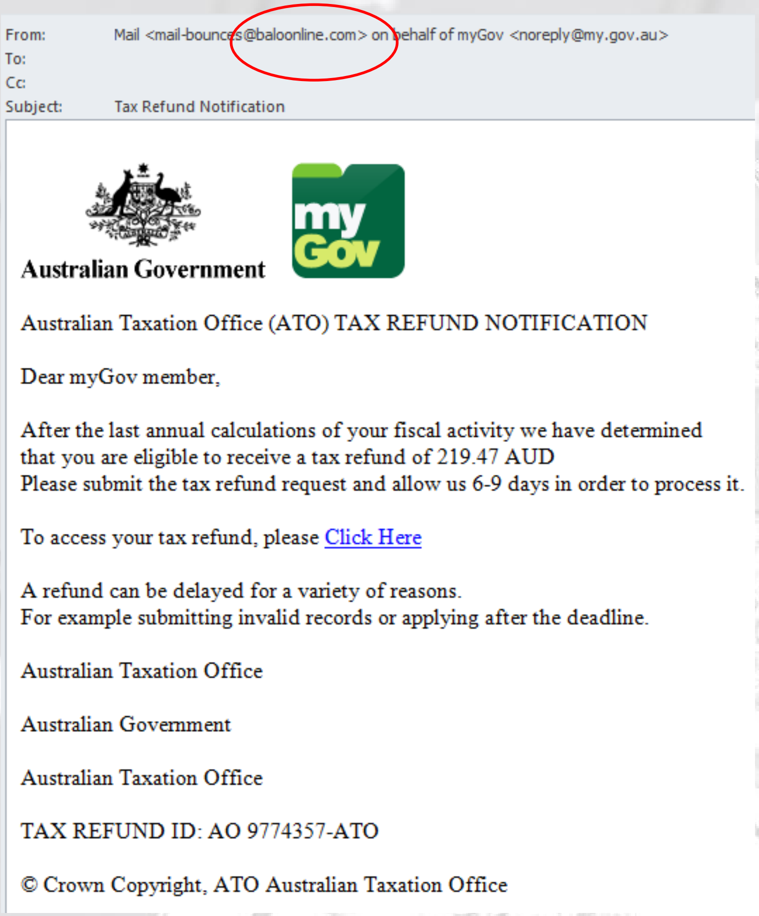
https://www.amazon.com/userdata/accounts/security/fraud-prevention

https://bit.ly/2XCDhQD

amazon

Copyright 2019 Amazon.com, Inc All rights reserved.

We hope you found this message to be useful. However, if you'd rather not receive future e-mails or this sort from Amazon, please visit the opt-out link below
https://www.amazon.com/gp/gss/o/4337ddfds.32hdhd



From: Mail <mail-bounces@baloonline.com> on behalf of myGov <noreply@my.gov.au>
To:
Cc:
Subject: Tax Refund Notification

Australian Taxation Office (ATO) TAX REFUND NOTIFICATION

Dear myGov member,

After the last annual calculations of your fiscal activity we have determined that you are eligible to receive a tax refund of 219.47 AUD
Please submit the tax refund request and allow us 6-9 days in order to process it.

To access your tax refund, please Click Here

A refund can be delayed for a variety of reasons.
For example submitting invalid records or applying after the deadline.

Australian Taxation Office

Australian Government

Australian Taxation Office

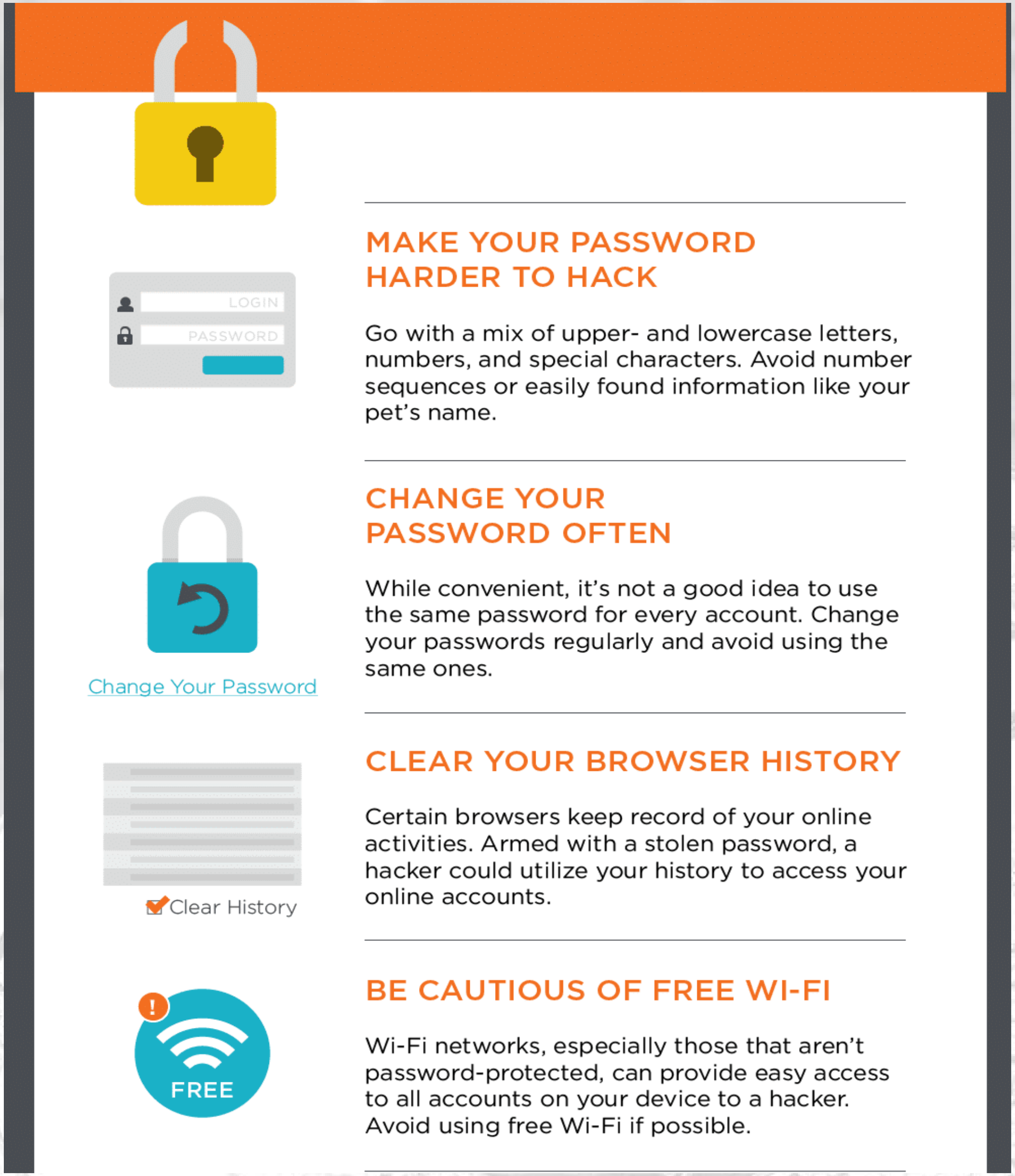
TAX REFUND ID: AO 9774357-ATO

© Crown Copyright, ATO Australian Taxation Office

If in doubt, go directly to the source and ask questions – do not click on any links

District 9810 Help…

PROTECT YOURSELF FROM HACKING


LOGIN
PASSWORD
Change Your Password
Clear History
FREE

MAKE YOUR PASSWORD HARDER TO HACK

Go with a mix of upper- and lowercase letters, numbers, and special characters. Avoid number sequences or easily found information like your pet's name.

CHANGE YOUR PASSWORD OFTEN

While convenient, it's not a good idea to use the same password for every account. Change your passwords regularly and avoid using the same ones.

CLEAR YOUR BROWSER HISTORY

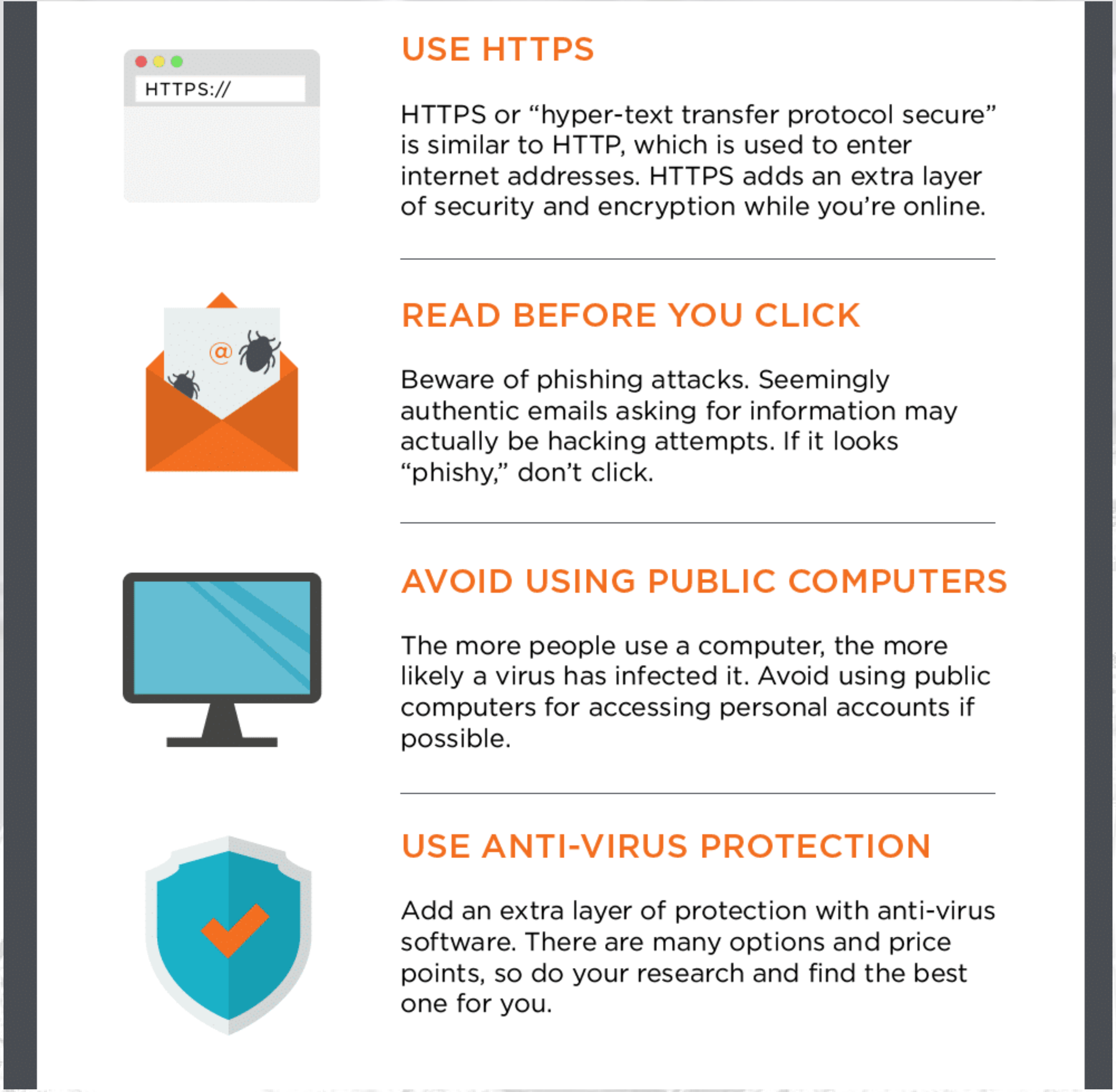
Certain browsers keep record of your online activities. Armed with a stolen password, a hacker could utilize your history to access your online accounts.

BE CAUTIOUS OF FREE WI-FI

Wi-Fi networks, especially those that aren't password-protected, can provide easy access to all accounts on your device to a hacker. Avoid using free Wi-Fi if possible.

PROTECT YOURSELF FROM

HACKING



USE HTTPS

HTTPS or “hyper-text transfer protocol secure” is similar to HTTP, which is used to enter internet addresses. HTTPS adds an extra layer of security and encryption while you’re online.

READ BEFORE YOU CLICK

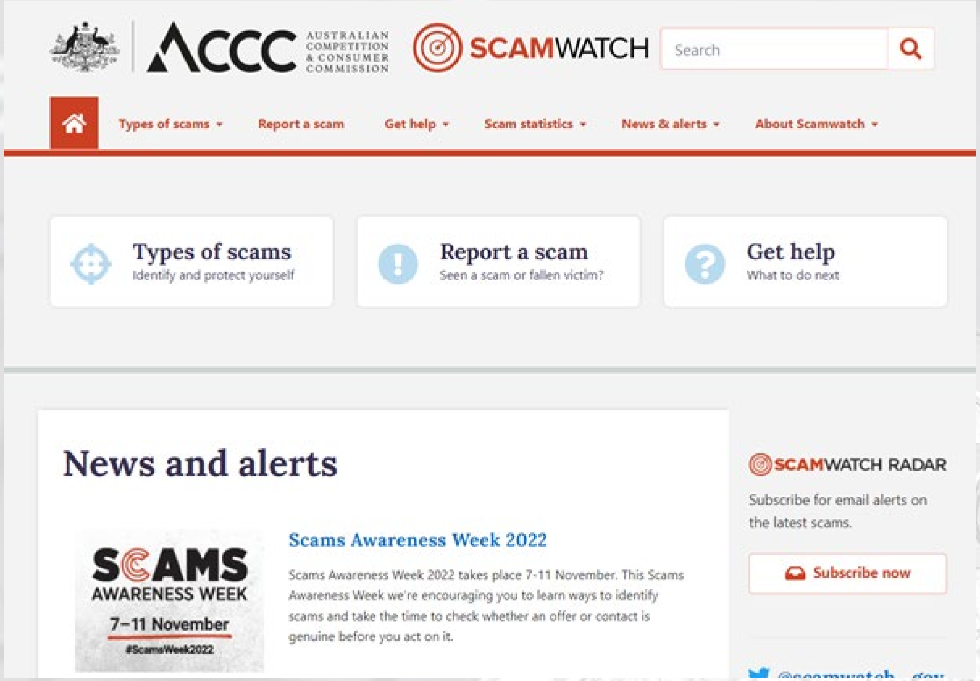
Beware of phishing attacks. Seemingly authentic emails asking for information may actually be hacking attempts. If it looks “phishy,” don’t click.

AVOID USING PUBLIC COMPUTERS

The more people use a computer, the more likely a virus has infected it. Avoid using public computers for accessing personal accounts if possible.

USE ANTI-VIRUS PROTECTION

Add an extra layer of protection with anti-virus software. There are many options and price points, so do your research and find the best one for you.



Types of scams
Identify and protect yourself

Report a scam
Seen a scam or fallen victim?

Get help
What to do next

News and alerts

Scams Awareness Week 2022

Scams Awareness Week 2022 takes place 7-11 November. This Scams Awareness Week we're encouraging you to learn ways to identify scams and take the time to check whether an offer or contact is genuine before you act on it.

SCAMWATCH RADAR

Subscribe for email alerts on the latest scams.

Keep a look out on trusted sights like Scamwatch.

Check your online banking messages as they often add notes about scams

If in doubt check it out!