How to protect yourself and your small business when working from home

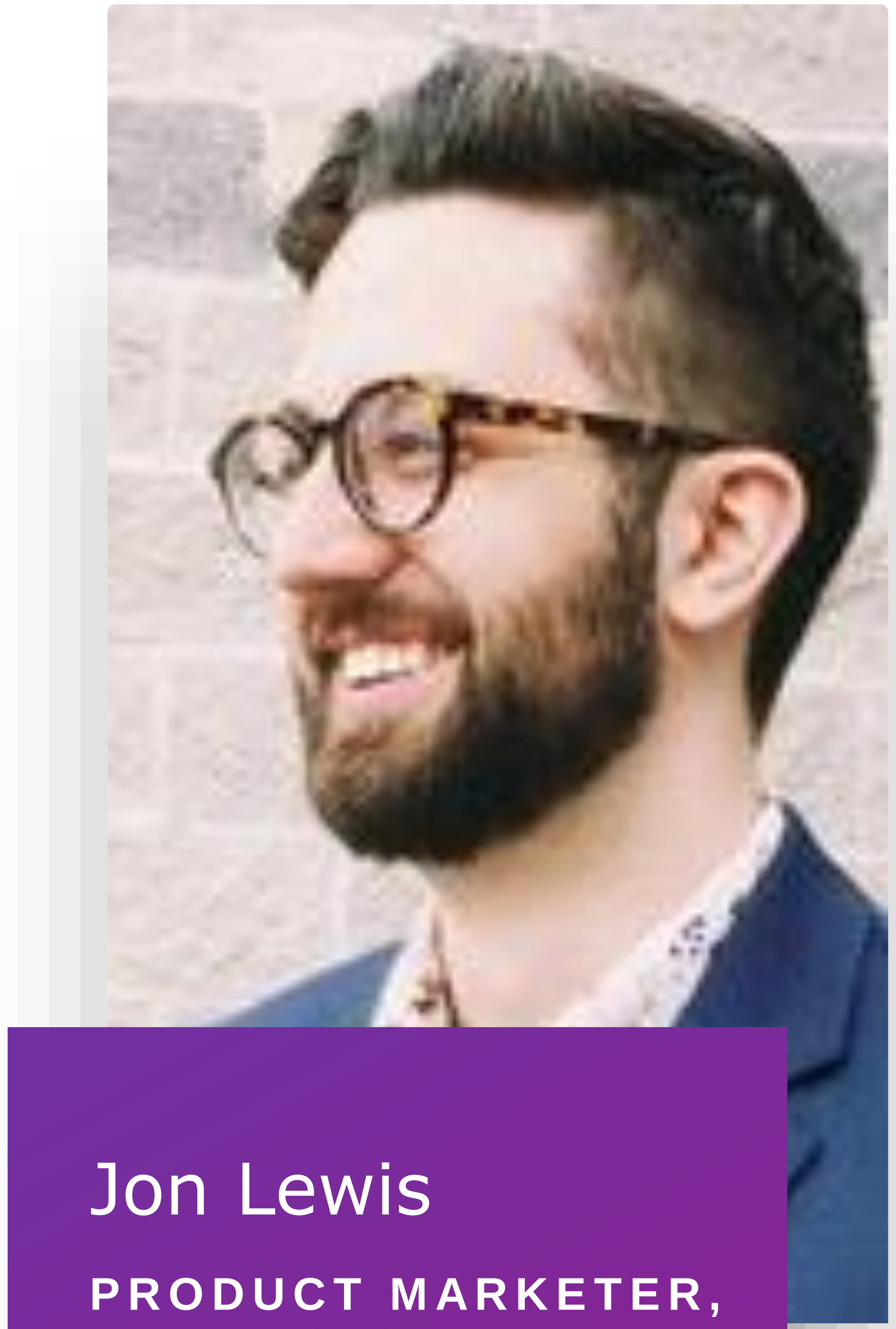
cira webnames.ca®

webnames.ca

Canada’s leading corporate domain registrar. For over 20 years now, we’ve helped Canadian professionals, small businesses and corporations secure their identities online.

cira

The domain registry that manages .CA domains, CIRA is a not for profit that supports and protects Canada’s internet.



Jon Lewis

PRODUCT MARKETER, CIRA

.CA

2.8 million .CA domains with 100% uptime.

Cybersecurity Services

1.8 million Canadians protected by D-Zone DNS Firewall

Registry Services

11% of country TLDs use our DNS services

W W W . C I R A . C A

We support initiatives that enhance Canadians' internet experience:

Global Internet Leadership

Support internet governance and standards through global organizations such as ICANN and CENTR

Canadian Initiatives

- **12** Internet Exchange Points nation-wide
- **120,000+** internet performance tests conducted last year

Community Initiatives

More than **$6.7 million** in grants to **151** projects through our Community Investment Program

What’re we talking about today?

- Why cybersecurity matters, even for families and households
- What cybersecurity risks come with WFH and COVID-19
- Simple tips to protect yourself (or your employees) at home
- Some freebies to take with you

Cyber attacks aren't just for big businesses

You can lose access to your accounts

Your identity can be leaked or stolen

Your money can be stolen

Your reputation can be hurt

Your devices can be held for ransom

Your devices can compromise others

COVID-19 threats

Dedicated cyber attacks related to or taking advantage of COVID-19

Remote work threats

General risks that are new, or are amplified, by working from home

COVID-19 cyber threats

Amplified attacks on critical infrastructure

Businesses going online for first time

People are psychologically compromised

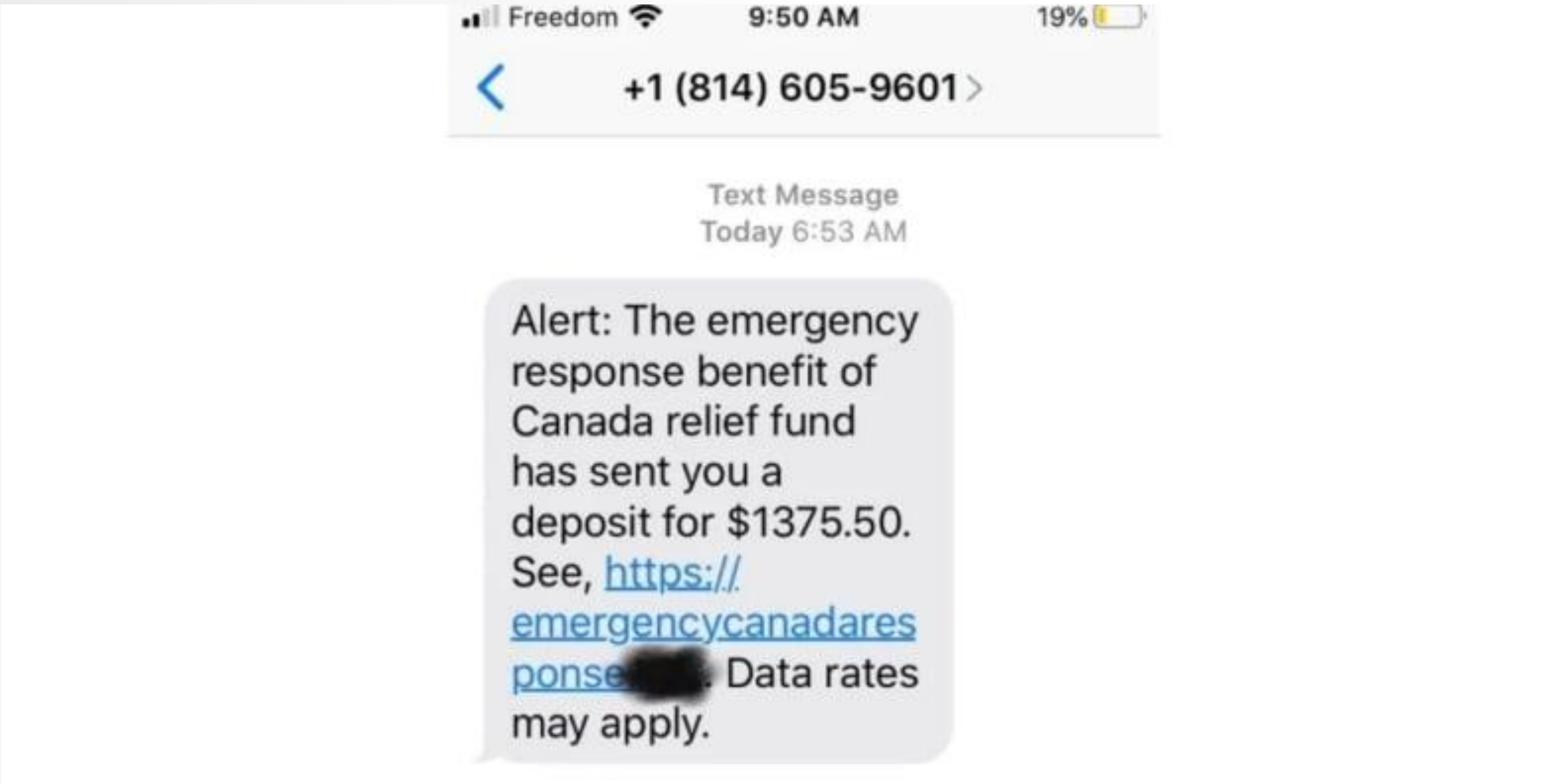
Malicious websites and domains

Misinformation on social media

New phishing emails, texts and calls

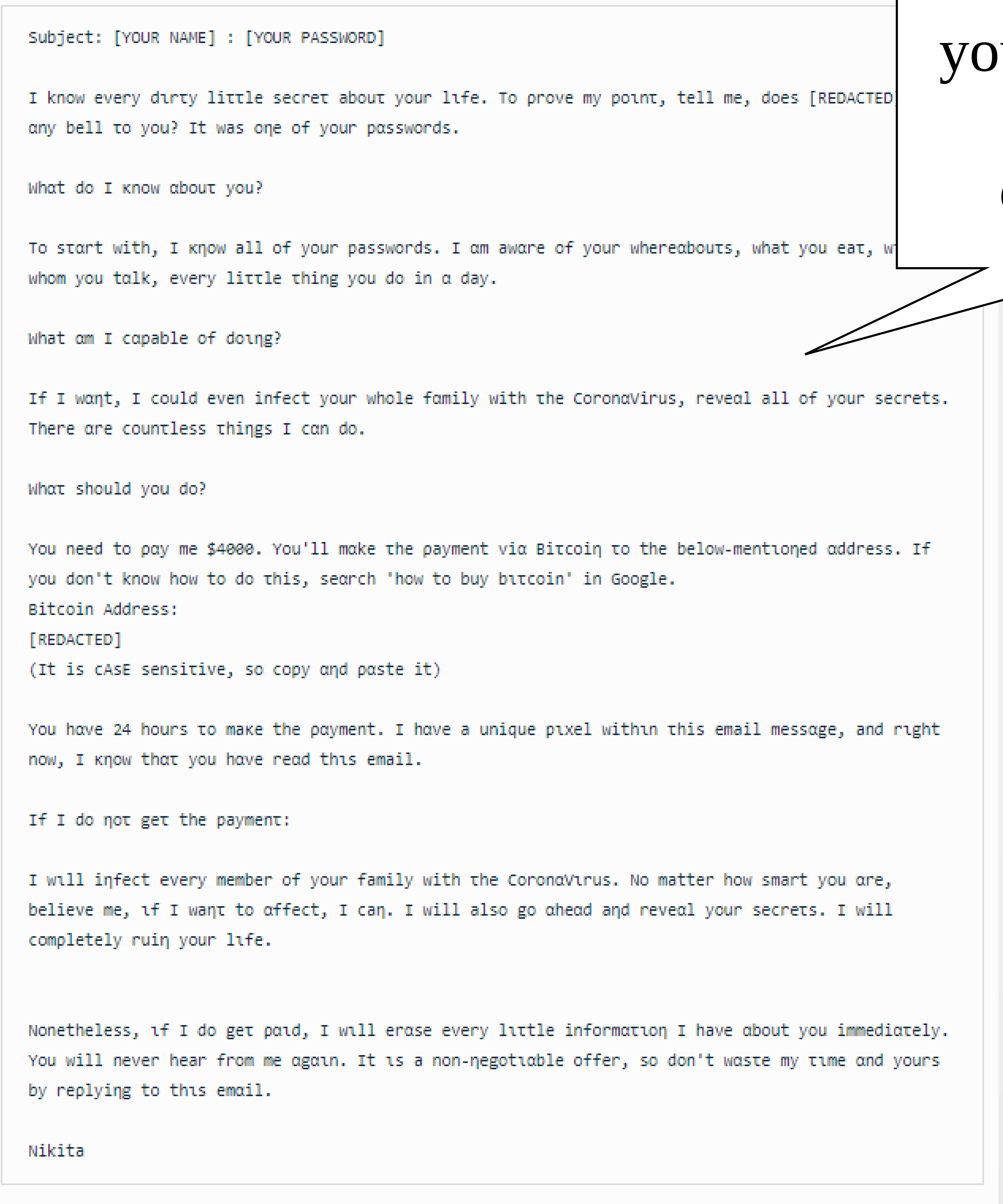
COVID-19 phishing scams

- Financial relief
- Charity/donations
- COVID-19 tests or health results
- Cleaning services
- Utilities



Text Message
Today 6:53 AM

Alert: The emergency response benefit of Canada relief fund has sent you a deposit for $1375.50. See, https://emergencycanadaresponse[redacted] Data rates may apply.



Subject: [YOUR NAME] : [YOUR PASSWORD]

I know every dirty little secret about your life. To prove my point, tell me, does [REDACTED any bell to you? It was one of your passwords.

What do I know about you?

To start with, I know all of your passwords. I am aware of your whereabouts, what you eat, w whom you talk, every little thing you do in a day.

What am I capable of doing?

If I want, I could even infect your whole family with the CoronaVirus, reveal all of your secrets. There are countless things I can do.

What should you do?

You need to pay me $4000. You'll make the payment via Bitcoin to the below-mentioned address. If you don't know how to do this, search 'how to buy bitcoin' in Google.
Bitcoin Address:
[REDACTED]
(It is cAsE sensitive, so copy and paste it)

You have 24 hours to make the payment. I have a unique pixel within this email message, and right now, I know that you have read this email.

If I do not get the payment:

I will infect every member of your family with the CoronaVirus. No matter how smart you are, believe me, if I want to affect, I can. I will also go ahead and reveal your secrets. I will completely ruin your life.

Nonetheless, if I do get paid, I will erase every little information I have about you immediately. You will never hear from me again. It is a non-negotiable offer, so don't waste my time and yours by replying to this email.

Nikita

“I could even infect your whole family with the Coronavirus”

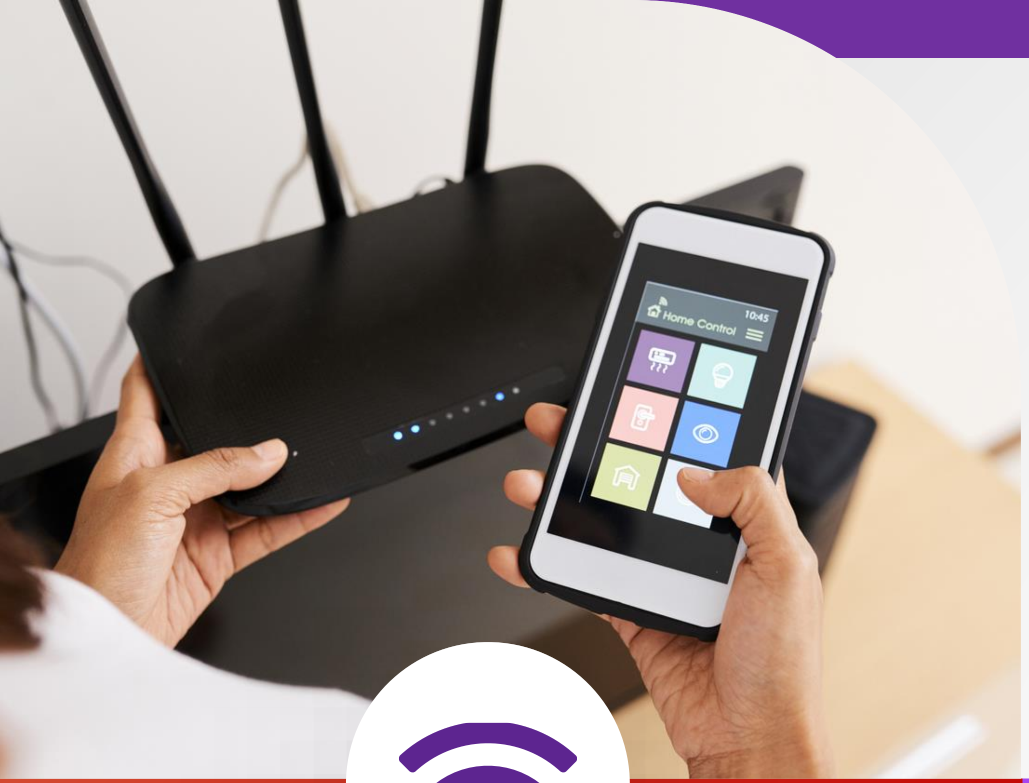
A traditional sextortion email with a twist

New challenge in cybersecurity:

Remote workers

Many organizations are forced to face remote work for the first time. Training has never been more important.

- Communicate consistently to a distributed workforce
- Compliance with new policies, like BYOD
- New process changes, like approving transactions
- Introduce new tools, like Zoom and Dropbox
- WFH brings new risks to educate
  - Personal networks aren’t as secure
  - Shared and personal devices

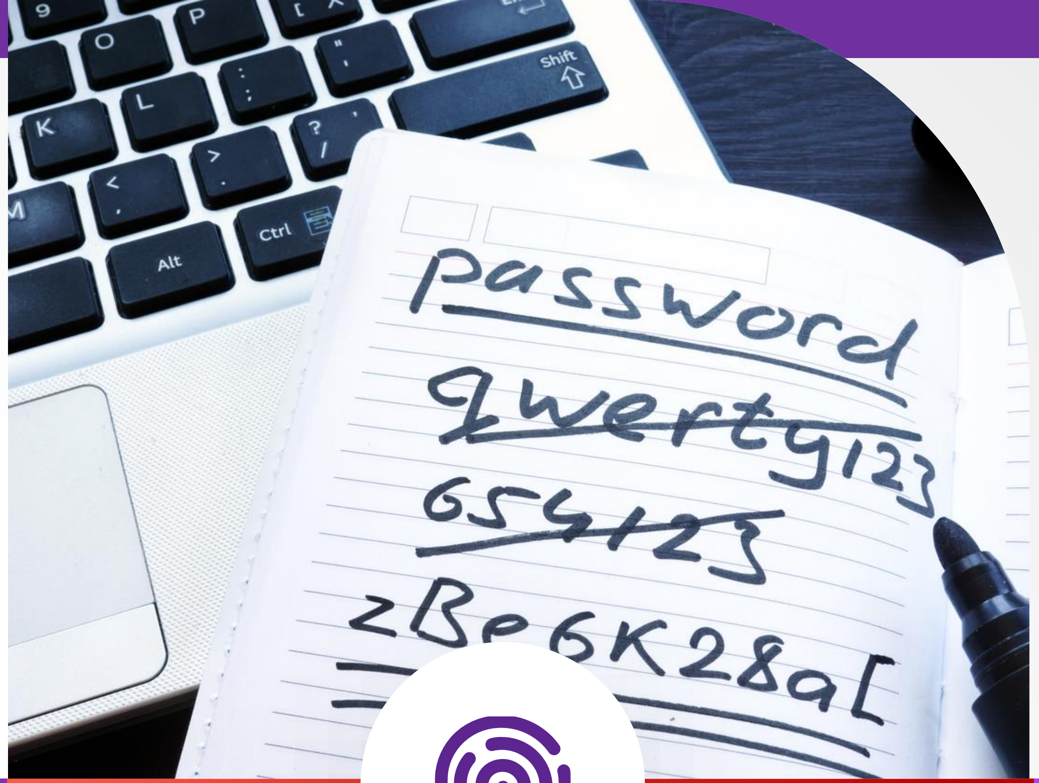


01

Protecting your personal Wi-Fi

Protecting your personal devices

02

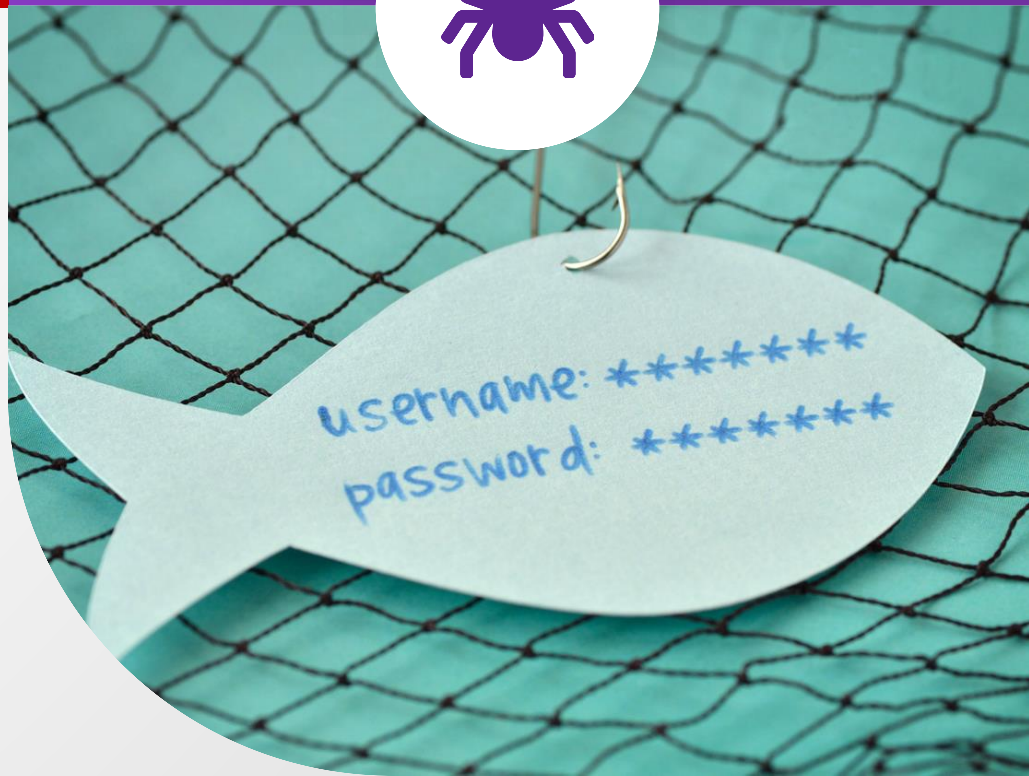


03

Practicing safe digital hygiene

Detecting phishing scams

04



cira

webnames.ca

1. Protect your Wi-Fi

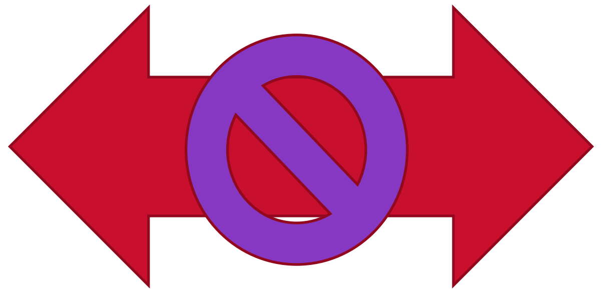
The most important part of your work-from-home setup is your Wi-Fi network.

A bad actor can use your Wi-Fi to access any device or information on your network.

✓ Change default router password
✓ Create a guest network
✓ Keep routers up to date
✓ Replace old routers
✓ Turn on WPA2 encryption
✓ Turn on a DNS protection service

Guest network

- Guest devices (like friends)
- Smart devices (like TVs and speakers)
- New, untested devices
- Old, not secured devices
- Children's devices



Hidden network (or VPN)

- Work devices
- Work phones
- Personal laptops and phones – may cause issues with smart devices

CIRA Canadian Shield

Turn on DNS protection

DNS is how your web browser looks up websites. Hackers can use the DNS to trick you into visiting fake websites, or to turn on the bad code they've tricked you into downloading.

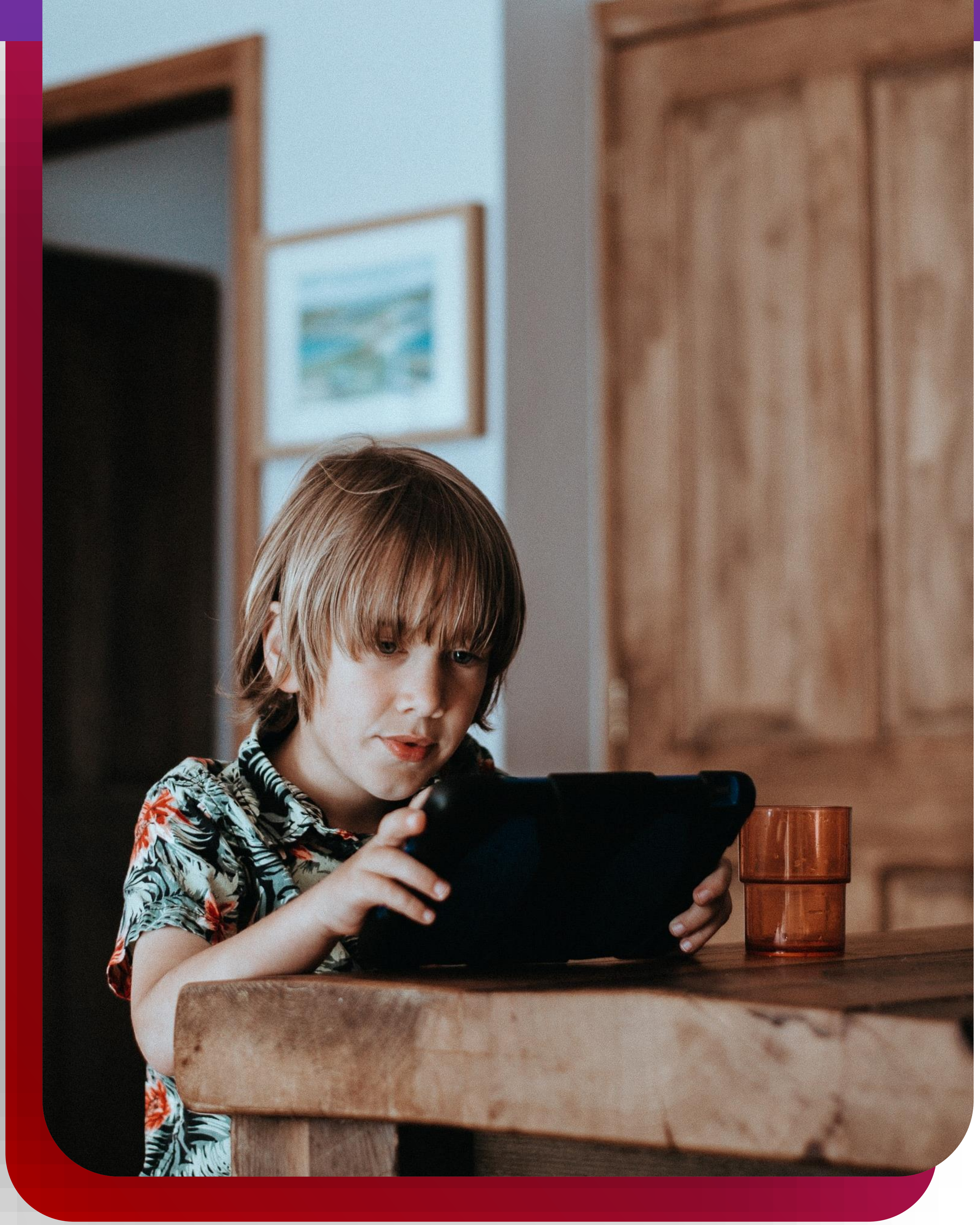
A DNS service designed for security checks the websites you're visiting against a list of known bad web domains.

✓ Log in to your router

✓ Go to "DNS settings"

✓ Change that number to our number

✓ Protects all devices on your network



2. Protect personal devices

If you use a compromised personal device to access work systems, you can put others at risk.

Be careful when sharing devices with others – do you know what they are downloading or visiting?

✓ Always update your devices

✓ Don’t share work devices with others

✓ Lock or turn-off devices when not in use

✓ Have file and device backups

✓ Only download apps from approved stores

✓ Use anti-virus software

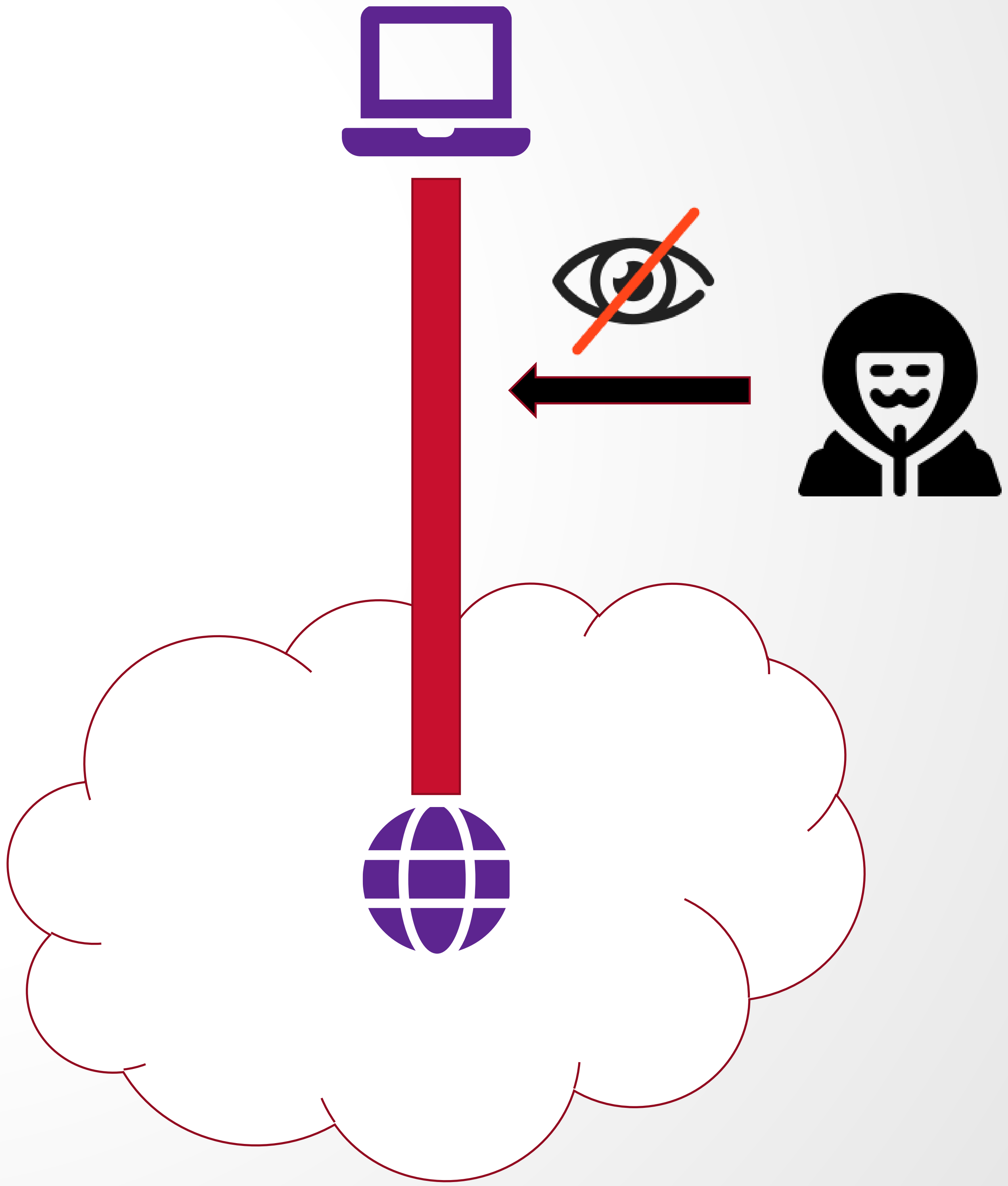
✓ Use a VPN to access important systems

What is a VPN? Virtual Private Network

A VPN is a **secure** connection to the internet.

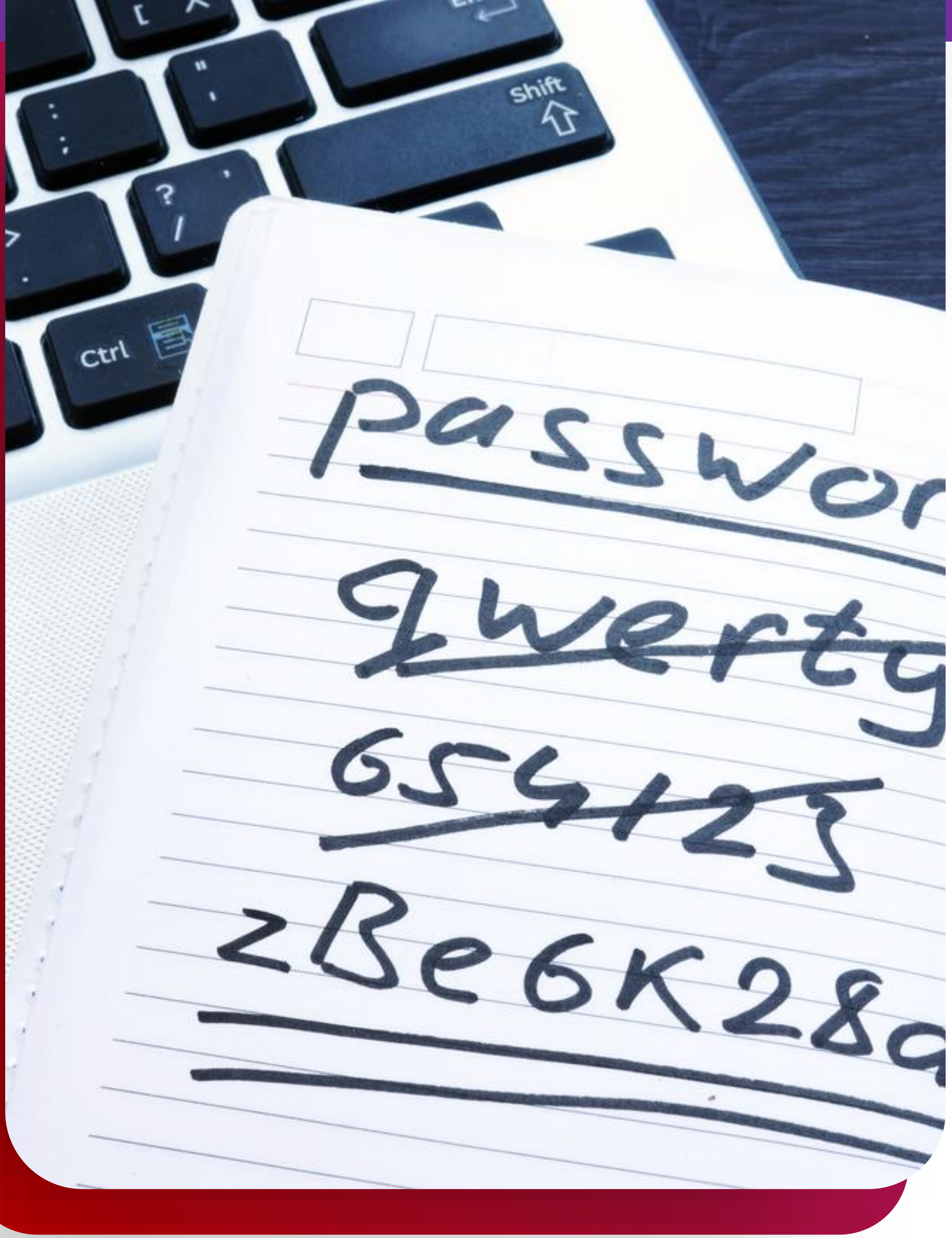
✓ Hides your identity on the internet

✓ Encrypts your internet behaviour



When to use a VPN:

- Using personal devices for work stuff
- Using public Wi-Fi



3. Digital hygiene

Hygiene is everything you to do clean-up and secure your online self.

Every surface you have on the internet can become a point of attack. Secure everything you can, both in personal and in work.

✓ Create strong, unique passwords
✓ Use a password manager
✓ Delete old accounts
✓ Turn on multi-factor authentication
✓ Unsubscribe from junk emails

Use a strong, long, unique password

******** = 5 hours

************ = 200 years

- Long (15+ characters recommended)
- Special characters (%, &, @)
- Avoid patterns (like asdf, 123)
- Avoid personal words (like birthdays, pets names)
- Avoid substitutions (like zero and O)

Make your life easier with a password manager

✓ Creates strong passwords for you

✓ Auto-populate – never remember a login again

✓ Works on your computer and phone

✓ Personal accounts are often free

Make your life easier with a password manager

- ✓ Creates strong passwords for you
- ✓ Auto-populate – never remember a login again
- ✓ Works on your computer and phone
- ✓ Personal accounts are often free
- ✓ Easy way to manage shared passwords for teams or families
- ✓ Store other important information, like security answers
- ✓ Makes moving to new devices easier

LastPass•••|

1Password

NordPass

DASHLANE

Multi-factor authentication (MFA)

You know when you get an email or text code to log in? That’s multi-factor authentication.

MFA means needing two or more of something you…

Know

(password, PIN number)

Have

(phone, email, authenticator app)

Are

(fingerprint, Face ID)

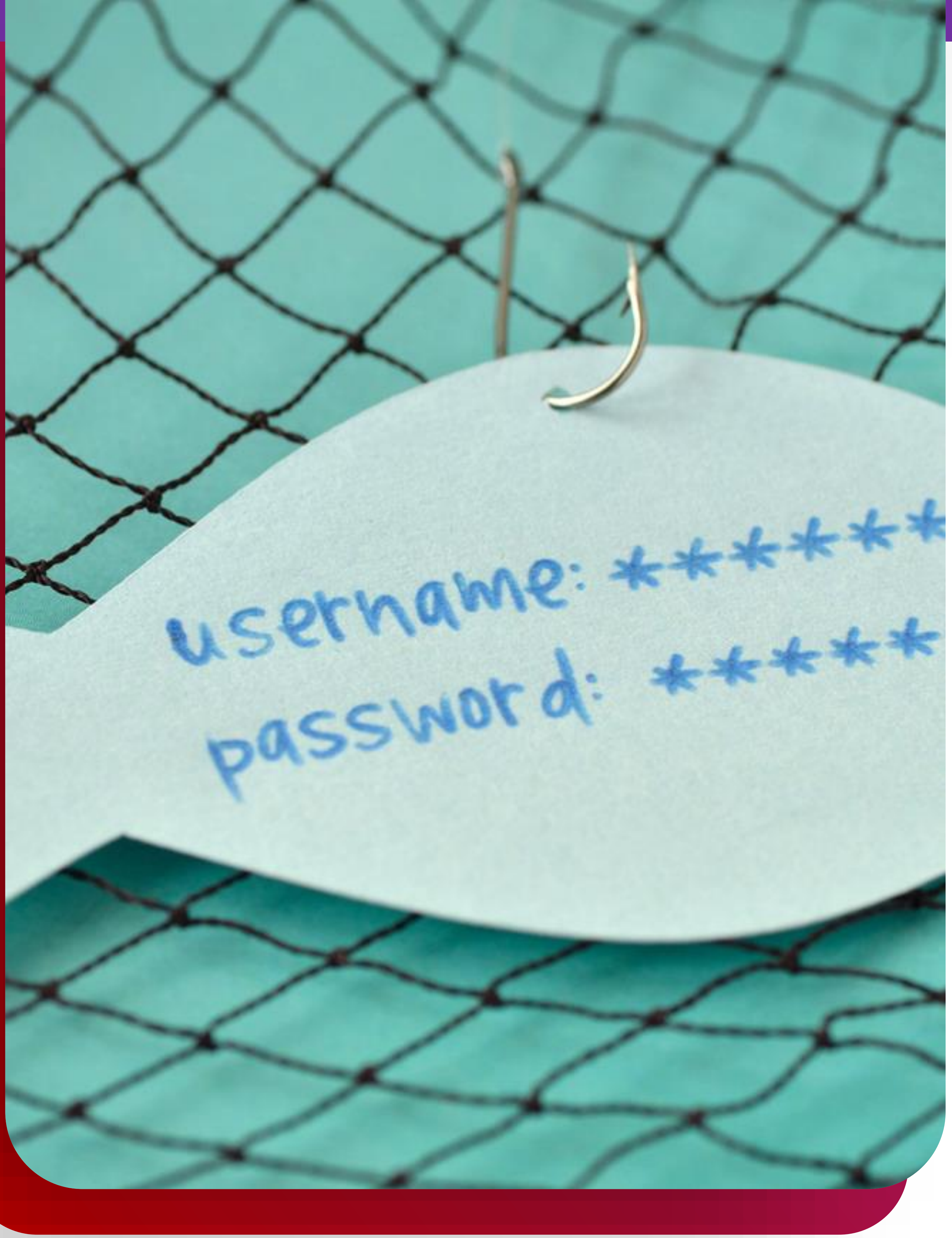
Digital hygiene for your website

✓ Turn on multi-factor authentication for your Webnames account and services

✓ Add an SSL certificate to your website

✓ Make strong, unique passwords for:

- Webnames account
- Website host/admin portal (like Wordpress)
- Email services
- Social media accounts



4. Phishing scams

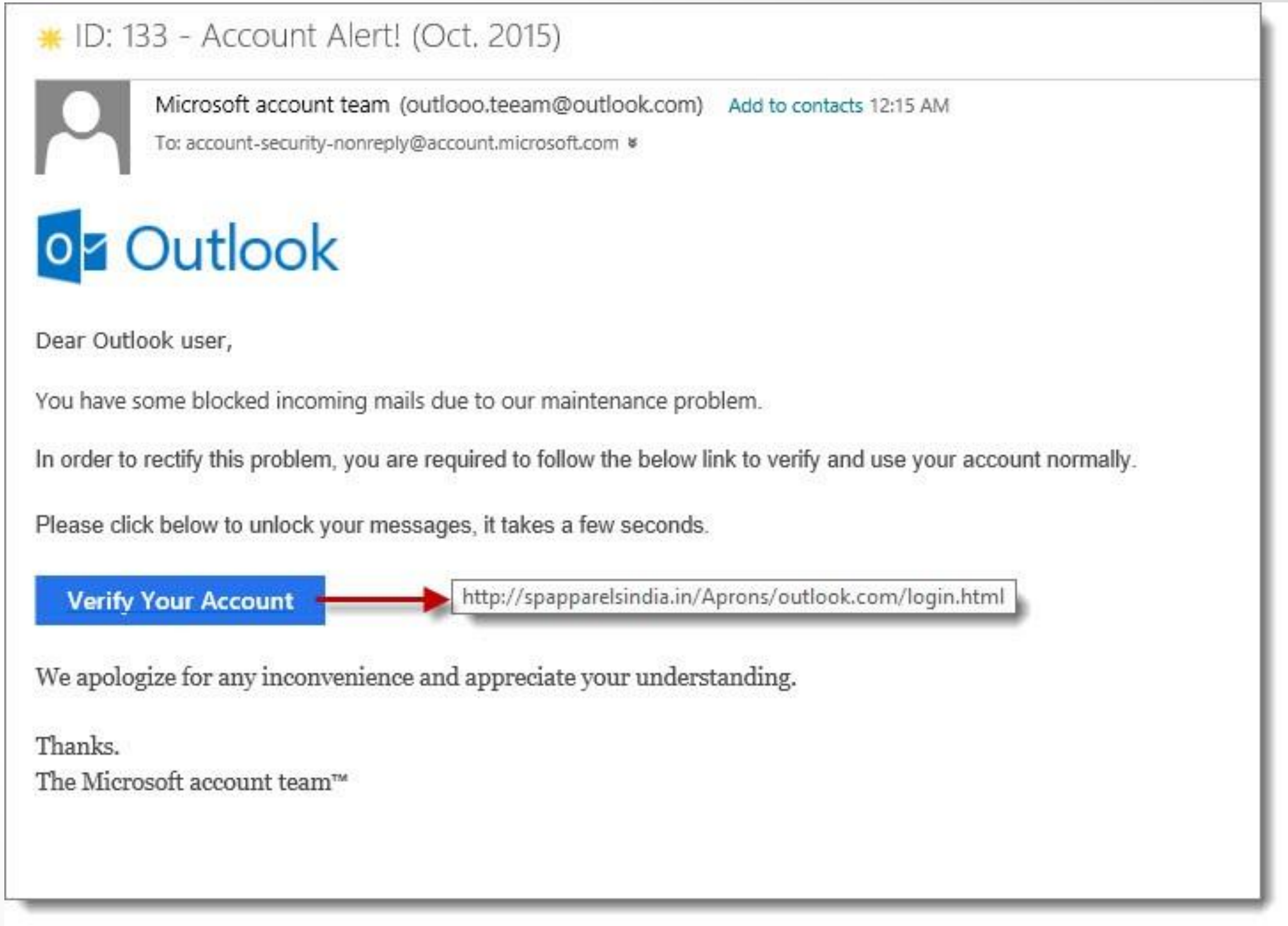
Phishing is when someone tries to impersonate others to steal your information, login credentials, or money.

Phishing can happen from email, text, calls, and social media.

Common phishes pretend to be the CRA, banks, police, your boss, or family members.

How to spot a phishing email

- Spelling errors
- Website isn’t the right one
- Strange email address and name
- Suspicious attachment
- Uses urgency or fear
- Seems too good to be true
- Threatening to arrest you
- Asks you not to tell others



ID: 133 - Account Alert! (Oct. 2015)

Microsoft account team (outlooo.teeam@outlook.com) Add to contacts 12:15 AM

To: account-security-nonreply@account.microsoft.com

Dear Outlook user,

You have some blocked incoming mails due to our maintenance problem.

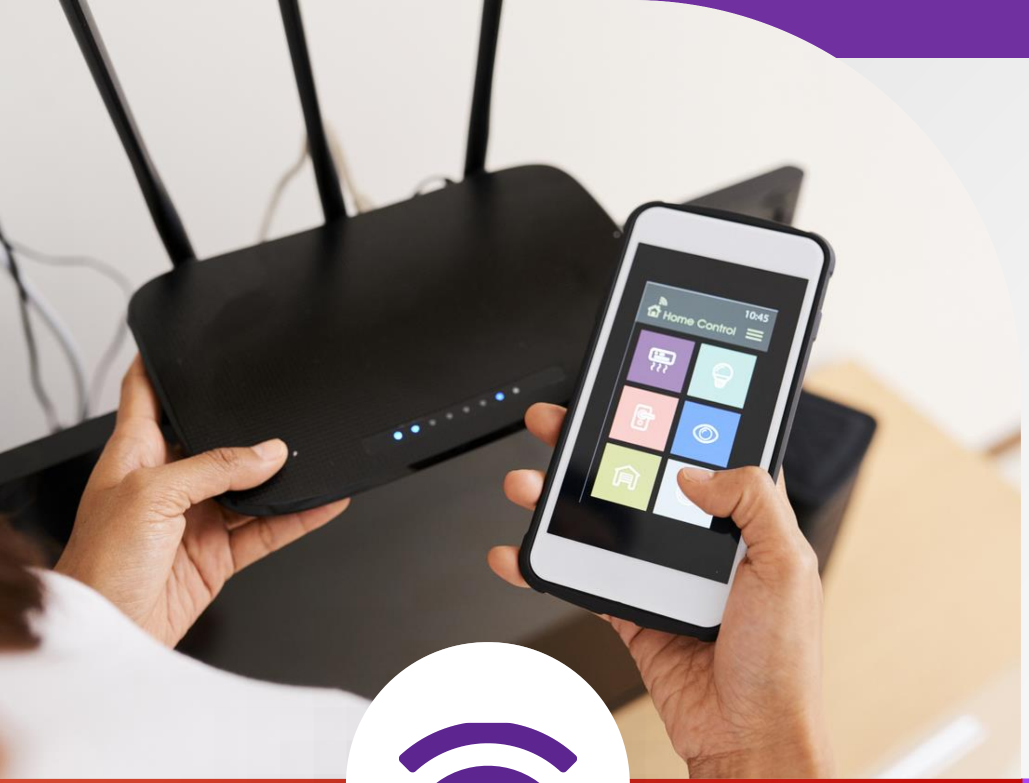
In order to rectify this problem, you are required to follow the below link to verify and use your account normally.

Please click below to unlock your messages, it takes a few seconds.

http://spapparelsindia.in/Aprons/outlook.com/login.html

We apologize for any inconvenience and appreciate your understanding.

Thanks.
The Microsoft account team™

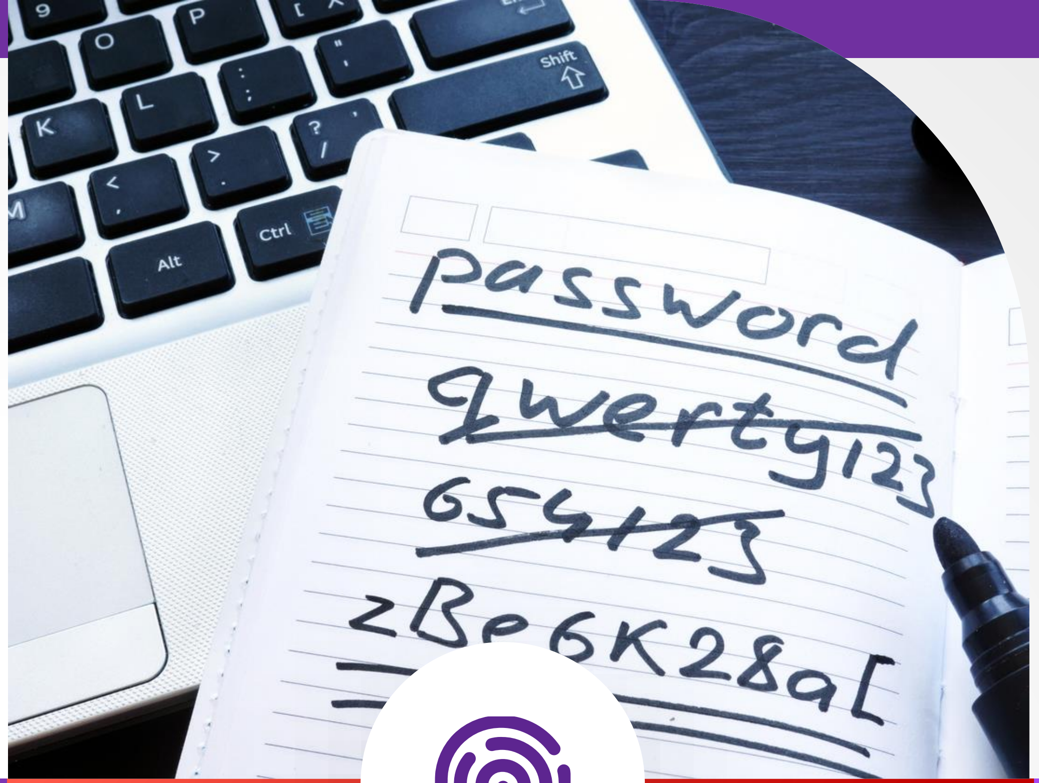


01

Protecting your personal Wi-Fi

Protecting your personal devices

02

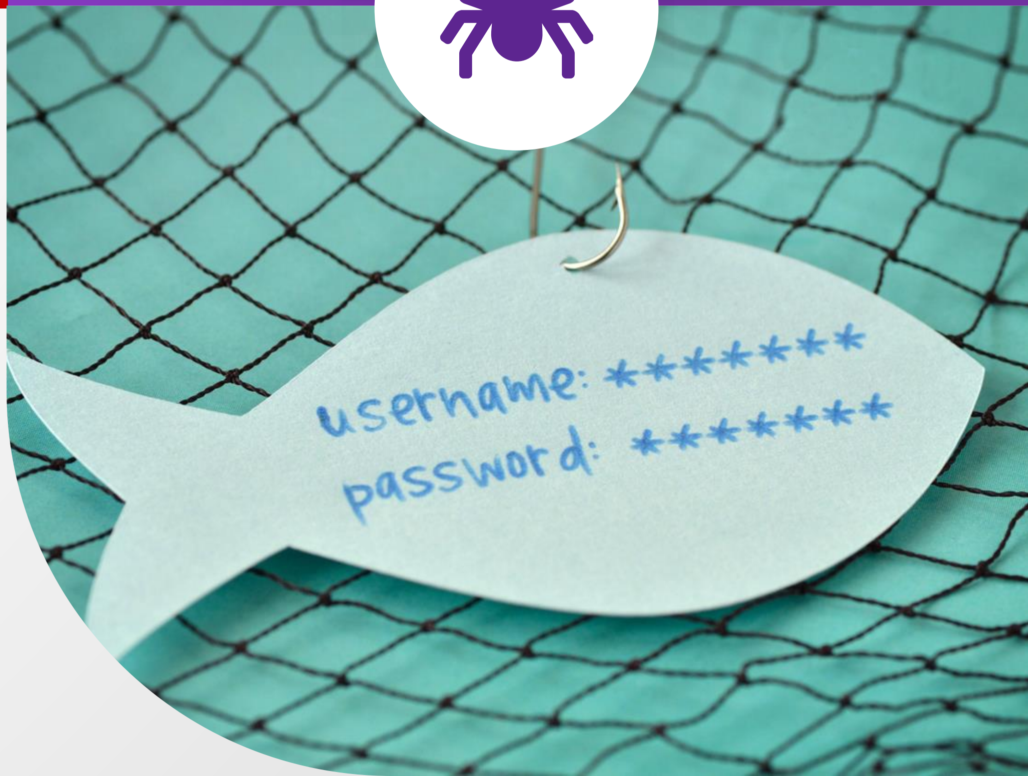


03

Practicing safe digital hygiene

Detecting phishing scams

04



cira webnames.ca

Next Steps

Free Cybersecurity Resources + Tools

Get Started: www.webnames.ca/**cybersecurity-tools**

WWW.CIRA.CA

Cybersecurity for Remote Workers

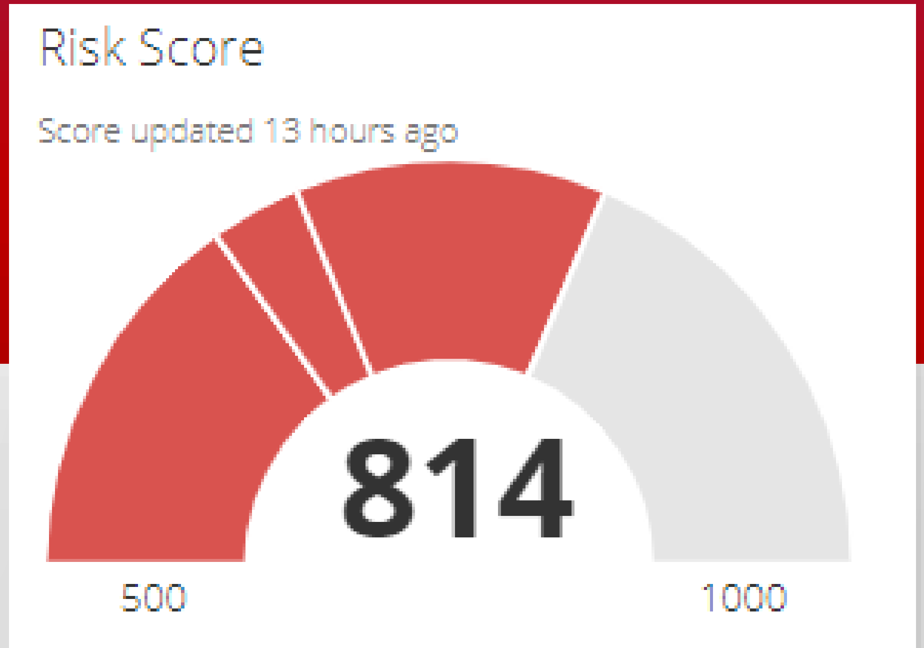
How to stay secure online when working from home

Free Course

Cybersecurity for remote workers

Canadian Shield

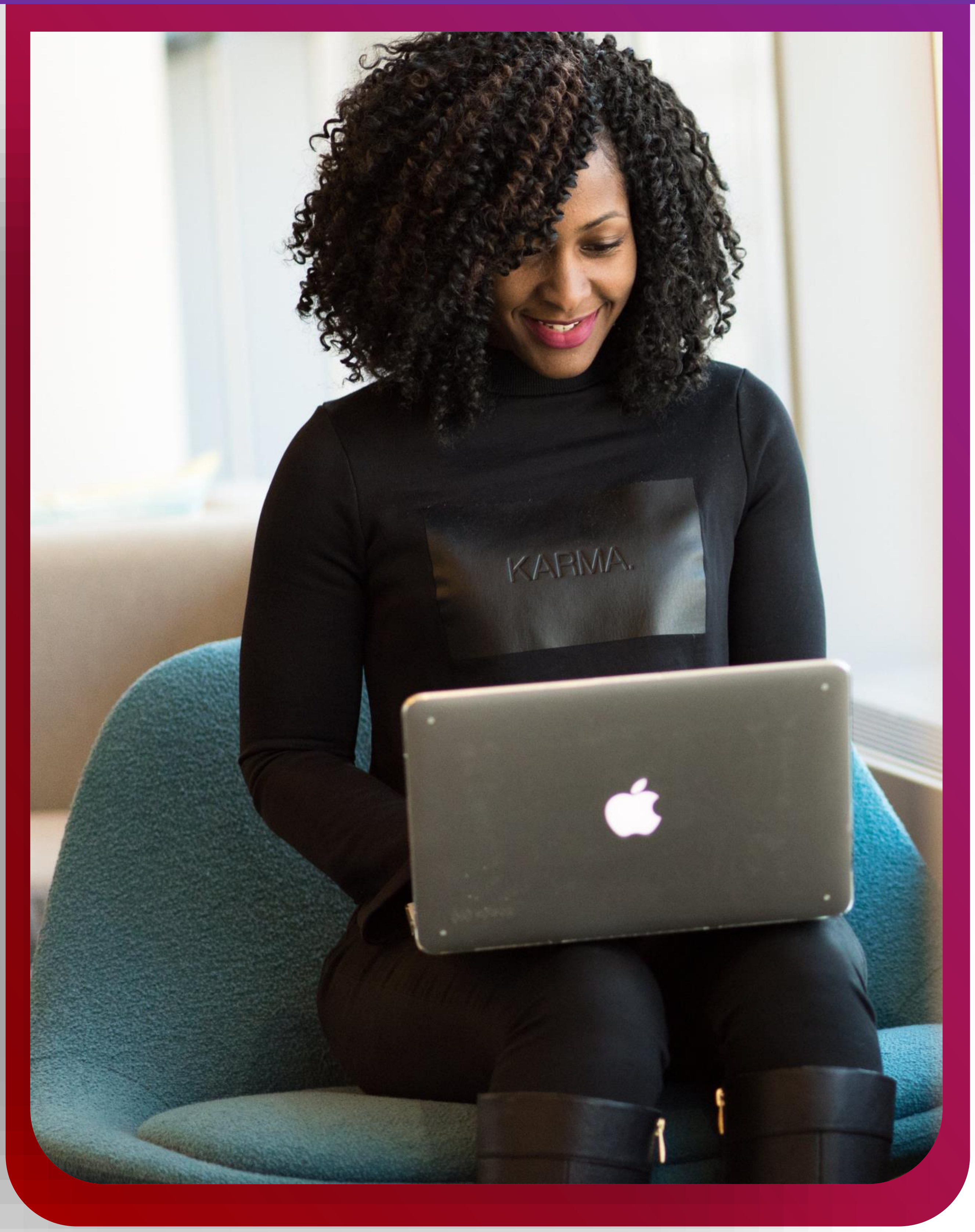
Free DNS service for households



Training Platform for IT Teams

Train and test staff to reduce phishing incidents

cira



Your turn.
Questions?

Thank you for joining us.

Have a question that didn't get answered today?

Need information about something this webinar touched on?

Contact us at **marketing@webnames.ca** for answers.

webnames.ca/**cybersecurity-tools**