AIR CADET LEAGUE OF CANADA · 2026 EDITION

Cybersecurity Awareness

Spotting today's phishing and protecting your Microsoft 365, Outlook and Gmail accounts

K2E Security

Why this matters in 2026

8.3 billion

phishing emails detected by Microsoft in the first three months of 2026

Microsoft Threat Intelligence

86%

of phishing attacks are now written or enhanced with AI

KnowBe4, 2026

$704M

lost to fraud by Canadians in 2025, and only 5–10% of fraud gets reported

Canadian Anti-Fraud Centre

Today's goals

Recognize 2026 phishing

QR codes, fake CAPTCHAs, device codes, AI-written emails

Lock down your accounts

Strong passphrases and two-step verification

Know what to do

How to report, and what to do if you already clicked

PART 1

Phishing and social engineering

Attackers hack people, not just computers

Social engineering tricks you into handing over information, money or access. Phishing is its most common form, and it now arrives through every channel.

- **Email** Phishing
- **Text message** Smishing
- **Phone call** Vishing, now with AI-cloned voices
- **QR code** Quishing
- **Teams and calendar invites** Fake meetings and shared files

The emotional levers they pull

Urgency
“Your account closes in 24 hours”

Fear
“Unpaid invoice”, “legal notice”, “suspicious sign-in”

Greed
“You've won a gift card”

Curiosity
“See who shared a file with you”

Empathy
“A cadet’s family urgently needs help”

Check three things in every message

A phishing email can look like it comes from someone you trust. Slow down and check these before you act.



Sender

Who is really sending this?

- Is it from our organization's real domain?
- Is a colleague writing from a personal Gmail or Outlook.com address?
- Does the address match the display name?



Context

Why are they sending it?

- Were you expecting this message?
- Would this person normally ask this?
- Are they pushing you to act fast or keep it quiet?



Content

Does it make sense?

- Where do the links really go? Hover first.
- Is it asking for a password, code or payment?
- Is there an unexpected attachment, QR code or shared file?



Not sure? Contact the person using a phone number or address you already have, never the one in the message.

Check the sender's exact address

The display name can say anything. Always read the address after the “@”.

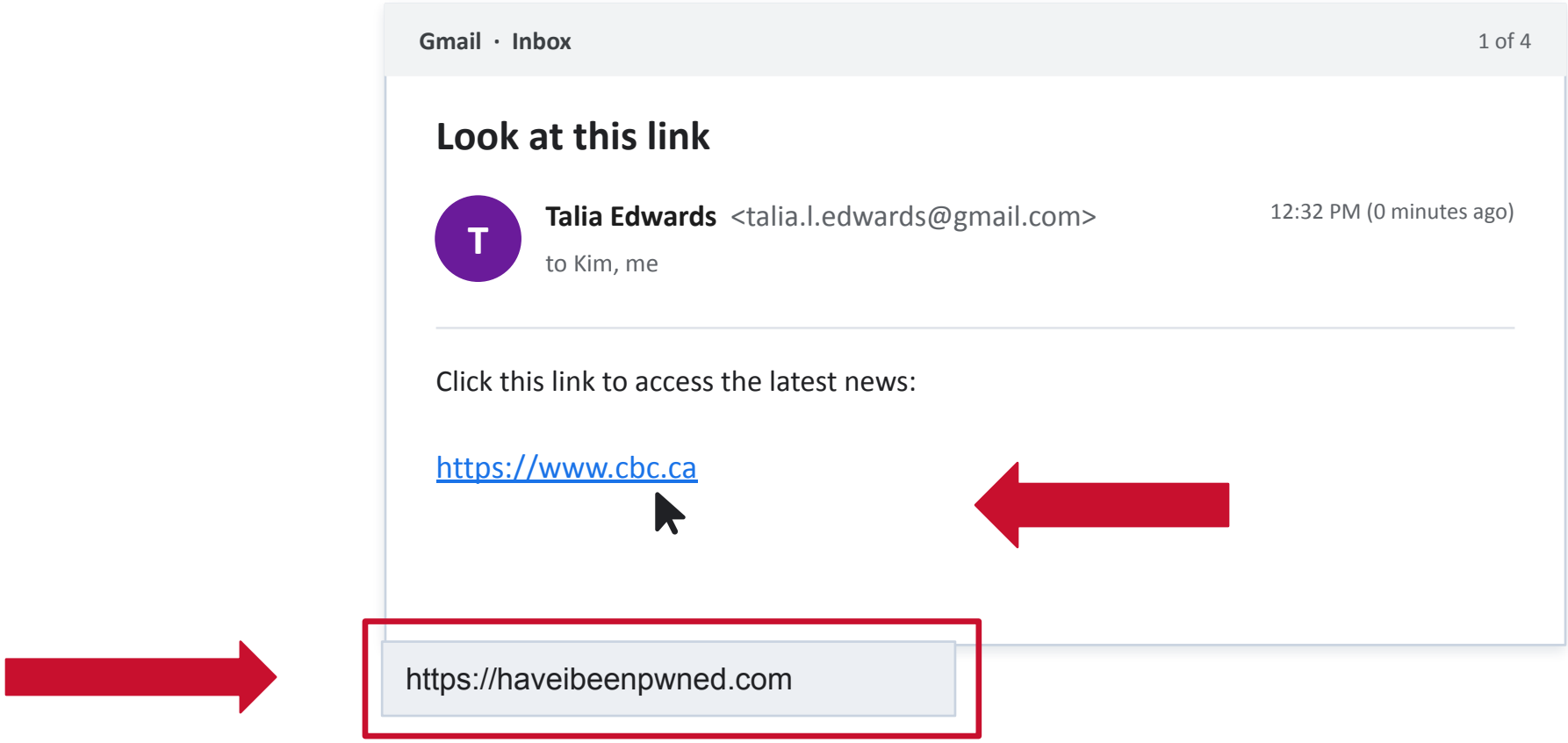
Type	What you see	Verdict
Official	`execdir@aircadetleague.com`	✓ **Legitimate**
Typosquat	`execdir@aircadet-league.com`	✕ **Fake: extra hyphen**
Extension swap	`execdir@aircadetleague.co`	✕ **Fake: missing “m”**
Look-alike letter	`execdir@aircadetIeague.com`	✕ **Fake: capital “I” instead of “l”**
Name spoof	`“Pierre Forgues” <pierre.forgues@gmail.com>`	✕ **Fake: personal account**

On your phone

Outlook and Gmail apps show only the name. Tap the sender's name to reveal the full address before you trust it.

A familiar name from a Gmail or unknown address is a red flag, even if it's the Executive Director's name.

How to hover over a link



The link says cbc.ca, but the hover preview at the bottom shows the real destination. They don't match, so don't click.

Hover before you click: read the real domain

Hover with your mouse, or press and hold on mobile. The real domain sits just before the first single “/”.

✓ SAFE

`https://login.microsoftonline.com/common/oauth2`

Real Microsoft sign-in domain. What comes after the “/” doesn't matter.

✕ FAKE

`https://login.microsoftonline.verify-acct.ru/`

Real domain is verify-acct.ru. “microsoftonline” is just a decoy.

✕ FAKE

`https://ACCOUNTS.GO0GLE.COM/signin`

A zero replaces an “o”. All caps makes it harder to spot.

Shortened links and QR codes hide the destination. If you can't see where it goes, don't open it.

PART 2

What's new: phishing tricks in 2026

Six phishing trends to know right now

AI-written phishing

86% of phishing is now AI-generated or AI-polished. Perfect spelling no longer means it's safe.

QR code phishing

Up 146% in early 2026. Scanning moves you to your phone, outside work protections.

Fake CAPTCHA (“ClickFix”)

A “prove you're human” page tells you to paste and run a hidden command.

Device codes and MFA bypass

You sign in on the real Microsoft page, but with the attacker's code, so they get in.

Calendar and Teams lures

Calendar-invite phishing up 49% and Teams attacks up 41% (KnowBe4).

Fake alerts and callbacks

Fake “Google security alert” emails, followed by calls from fake “support”.

Example: the “password expiring” QR code

Outlook · Inbox

1 **Action required: your password expires today**

Microsoft 365 Security <no-reply@m365-securenotice.com>

To: kim@aircadetleague.com

Hi Kim,

2 Your Microsoft 365 password expires today. To keep your current password, scan the code below with your phone.

This request expires in 2 hours.

3



1 **Look-alike sender**

Not microsoft.com. The display name is doing all the work.

2 **Urgency and an odd offer**

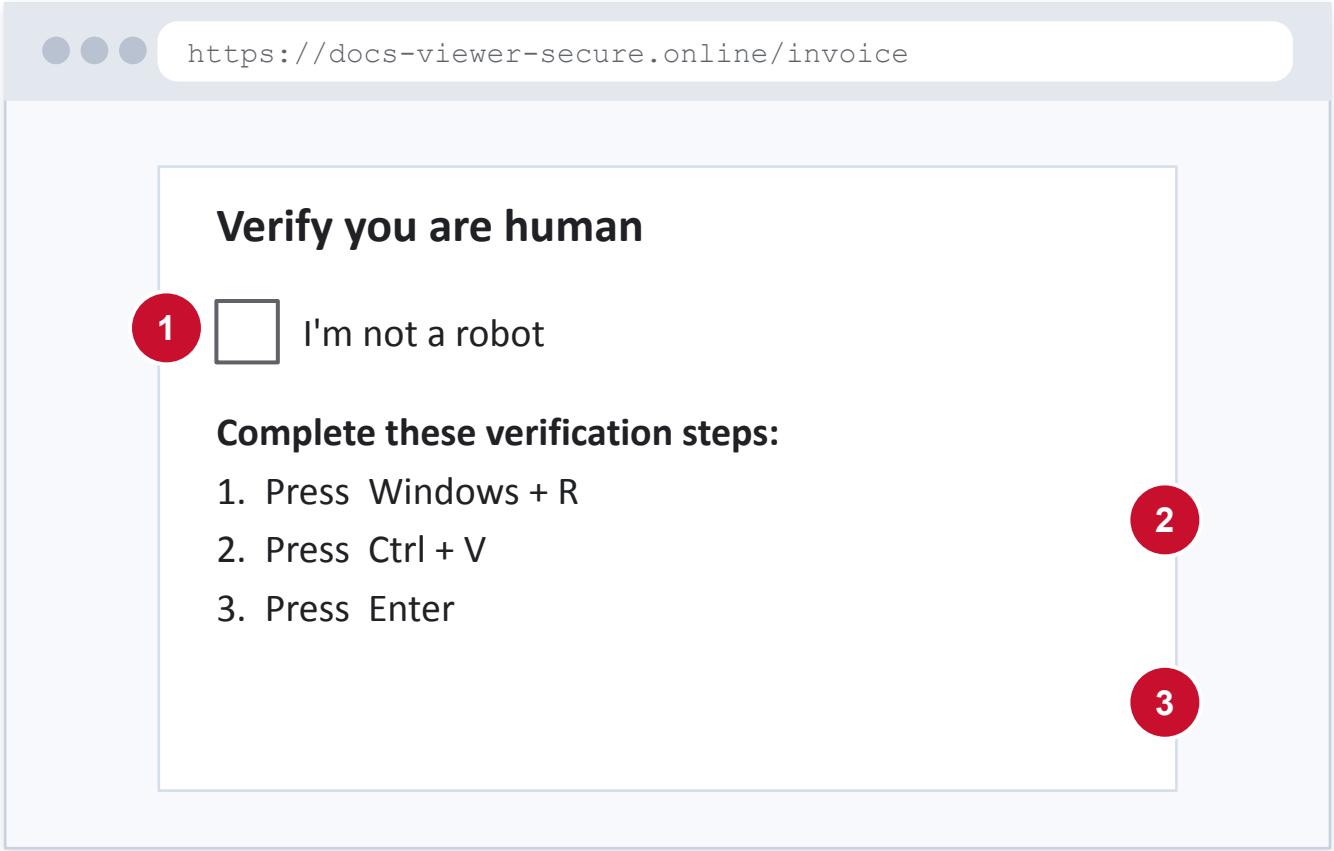
“2 hours” and “keep your current password” are classic pressure lines.

3 **The QR code is the trap**

It moves you to your phone, where you can't hover and work protections don't apply. QR phishing rose 146% in early 2026.

Never scan a QR code to sign in, “verify” or keep a password.

Example: the fake “I'm not a robot” check



1 Clicking the box copies a command

The page silently puts a malicious command on your clipboard.

2 The “steps” run it

Windows + R, paste and Enter launches it. On a Mac, the page asks you to paste into Terminal.

3 What it installs

Usually an info-stealer that grabs saved passwords and signed-in sessions, including Microsoft 365 and Gmail.

No real website ever asks you to paste anything into Run, PowerShell or Terminal. Close the tab.

Example: device-code phishing in Microsoft 365

The sign-in page is real, so checking the web address isn't enough. One 2026 campaign hit more than 340 organizations, including in Canada.

1 You get a “shared file”

“Kim shared Squadron Budget 2026.xlsx. To view it, enter code WQ7K-DM4P at microsoft.com/devicelogin.”

2 You sign in on the real page

You type the code on Microsoft's genuine site, then approve your MFA prompt as usual.

3 The attacker is now you

The code belonged to the attacker's device. They get your mailbox and OneDrive, no password needed.

Only enter a device code when you're setting up a TV, console or device that's right in front of you.

Example: the fake Google security alert

Gmail · Inbox

Security alert: a subpoena was issued for your Google Account

1 **Google** <no-reply@google.com>

To: kim.cadets@gmail.com

A law enforcement request requires us to share a copy of your account content. To review the request or file a protest, visit:

2 sites.google.com/view/support-case-48213

You have 48 hours to respond.

1 The address can look perfect

Attackers have replayed real Google messages so they show no-reply@google.com and pass Gmail's checks.

2 Anyone can build a sites.google.com page

A Google web address is not proof that Google made the page.

3 Then comes the phone call

Fake “Google” or “Microsoft support” calls and asks for the code sent to your phone.

Check alerts yourself at myaccount.google.com or account.microsoft.com, and never share a code with anyone.

Example: “Quick favour” and payment fraud

Outlook · Inbox

Quick favour

Maj. J. Tremblay <co.tremblay.squadron@gmail.com>

To: kim@aircadetleague.com

Are you available? I need you to pick up 5 x $100 gift cards for the cadet awards tonight.

I'm in meetings and can't take calls. Just email me photos of the card codes and I'll reimburse you tomorrow.

Sent from my iPhone

Spear phishing cost Canadians over **$68 million** in 2025, and about $31 million in just the first three months of 2026 (Canadian Anti-Fraud Centre).

Watch for

- A leader's name from a personal address
- Gift cards, wire transfers or e-Transfers
- “New banking details” from a supplier or vendor
- “I can't talk right now” and secrecy

Verify any payment request by phone, using a number you already have. Use two-person approval for squadron funds.

Report it, and act fast if you clicked

How to report

Outlook / Microsoft 365

Select the message, then Report > Report phishing.

Gmail

Open the message, then the ⋮ menu > Report phishing.

Suspicious texts

Forward the text to 7726 (SPAM) on any Canadian carrier.

Fraud or money lost

Canadian Anti-Fraud Centre: 1-888-495-8501 or online, plus your local police.

Already clicked or typed a password?

1. Don't panic, and don't hide it. Speed matters more than blame.
2. Change that password right away, from a device you trust.
3. Sign out of all sessions in your Microsoft or Google account security page.
4. Tell your squadron's IT contact or your supervisor.
5. If money or banking details were involved, call your bank now.

PART 3

Passwords and two-step verification

Make it long, make it unique

Most passwords are cracked because people follow predictable patterns. Length beats complexity.

✕ WEAK PASSWORD

Cracked in minutes by dictionary and brute-force attacks.

`AirCadets2024!`

organization name · year · symbol at the end

- ✕ Under 12 characters
- ✕ Built from names, years, seasons or pets
- ✕ Reused on other sites

✓ STRONG PASSPHRASE

Long and random, so it's far harder to crack.

`maple-ORBIT-tuesday-47canoe`

random words · one in CAPS · numbers · hyphens

- ✓ 12+ characters minimum, longer is better
- ✓ Random, unrelated words, not a quote or saying
- ✓ Unique to every account

Never use a password you've seen on a slide, including these examples.

Keep your passwords safe

Avoid

- ✕ Single dictionary words, or swaps like p@ssw0rd
- ✕ Names, birthdays, usernames or your squadron number
- ✕ Writing passwords on sticky notes
- ✕ Reusing one password everywhere
- ✕ Sharing passwords, even with coworkers

Do

- ✓ Use a password manager: Bitwarden, 1Password, or the one built into Google or Microsoft
- ✓ Use a passkey where it's offered: no password to steal
- ✓ Check whether your email was exposed at haveibeenpwned.com



Never share it

Not with coworkers, and never by email or chat.



Real sites only

Check the address bar before you type it.



Turn on two-step

A stolen password alone then isn't enough.



Exposed? Act now

Change it right away and tell your IT contact.

Turn on two-step verification today

Microsoft 365 and Outlook

Work or school account

Go to mysignins.microsoft.com/security-info > Add sign-in method > Microsoft Authenticator.

Personal Outlook.com

Go to account.microsoft.com/security > Manage how I sign in > turn on two-step verification.

Gmail and Google

Any Google account

Go to myaccount.google.com/security > How you sign in to Google > 2-Step Verification > Turn on.

Then add a backup

Add the Google Authenticator app or a passkey so you don't rely on text messages.

Which second step is best?

Passkey or security key

Strongest. Can't be phished.

Authenticator app

Strong. Uses number matching.

Text message code

Better than nothing.

How attackers try to get around MFA

MFA fatigue (push bombing)

With your password in hand, attackers send prompt after prompt, or call posing as IT, until you tap Approve just to make it stop.

Red flag: A prompt you didn't start, especially late at night.

Attacker-in-the-middle

A fake sign-in page passes your password and MFA approval to the real Microsoft or Google site in real time. Use of this technique rose 139% in 2026.

Red flag: The address bar doesn't show microsoft.com or google.com.

Read the prompt before you tap

Microsoft Authenticator asks you to type the number shown on your sign-in screen. Google shows the device and location. If there is no sign-in screen in front of you, or the details don't match, tap Deny, change your password and tell your IT contact.

PART 4

Devices, Wi-Fi and file sharing

Malware: how it gets in, and how to stop it

In 2026 the most common malware is the info-stealer: it quietly copies saved passwords and signed-in sessions. Ransomware locks your files and demands payment.

How it gets in

- Email attachments and shared files
- Fake CAPTCHAs and fake browser updates
- Pirated software, game mods and cracks
- Malicious ads and search results
- Unknown USB keys

Warning signs

- Pop-ups, or a new browser homepage
- Slow, crashing or overheating device
- Friends get messages you didn't send
- Password-reset emails you didn't request
- Unknown programs at startup

Protect yourself

- Turn on automatic updates
- Keep Microsoft Defender (Windows) or XProtect (Mac) on
- Install apps only from official stores
- Back up important files, including one offline copy
- Don't save passwords in a shared browser

Public Wi-Fi and file sharing

On public Wi-Fi

- Confirm the exact network name with staff: fake hotspots copy real names
- Use your phone's hotspot or a trusted VPN for sign-ins
- Turn off auto-join for open networks
- A padlock only means the connection is encrypted, not that the site is honest

When sharing files

- Use your organization's OneDrive, SharePoint or Google Drive, not personal accounts
- Share with specific people, not “Anyone with the link”
- Set an expiry date and remove access when you're done
- Never put cadet personal information on an unencrypted USB key

Cadet information is sensitive: share the minimum, with the fewest people, for the shortest time.

Eight habits that stop most attacks

- Check the sender's real address
- Hover before you click
- Never scan a QR code to sign in
- Never paste commands a website gives you
- Only enter codes you requested
- Long, unique passphrases and MFA
- Verify payment requests by phone
- Report it, even if you clicked

Questions?

K@K2ESEC.COM

When in doubt, don't click. Report it.



APPENDIX

Setup guides and references

For administrators and device owners

Microsoft 365 admins

- Require MFA for everyone: Microsoft Entra admin center > turn on security defaults, or use Conditional Access
- Block the device-code sign-in flow for users who don't need it (Conditional Access > Authentication flows)
- Turn on Safe Links, Safe Attachments and Zero-hour auto purge in Defender for Office 365

Google Workspace admins

- Admin console > Security > Authentication > 2-Step Verification > Allow users to turn on
- Have everyone enrol, then switch Enforcement on so no one is locked out
- Turn on Advanced Protection for admin and finance accounts

Check your own computer

- Windows: Start > Windows Security > Virus & threat protection. A green check means you're protected; make sure real-time protection is on
- Mac: System Settings > General > Software Update > Automatic updates > turn on “Install Security Responses and system files” (keeps XProtect current)

References

1. Microsoft Threat Intelligence, “Email threat landscape: Q1 2026 trends and insights” and “Q2 2026 trends and insights,” Microsoft Security Blog, 2026.
2. KnowBe4, “Phishing Threat Trends Report, Volume 7,” 2026.
3. Google, “Our latest fraud and scams advisory,” June 2026.
4. Proofpoint, research on Microsoft 365 device-code phishing, January and May 2026.
5. The Hacker News, “Device code phishing hits 340+ Microsoft 365 organizations,” March 2026.
6. Canadian Anti-Fraud Centre, “Top 10 frauds in 2025” and “Fraud Trends: First 6 Months of 2026.” antifraudcentre-centreantifraude.ca
7. Canadian Anti-Fraud Centre, news release on payment redirection fraud, May 13, 2026.
8. U.S. Federal Trade Commission, “How to spot a CAPTCHA scam,” June 2026.
9. Canadian Centre for Cyber Security, guidance on passphrases and multi-factor authentication. cyber.gc.ca