

How to Identify and Report Phishing Emails

Phishing emails are one of the biggest security threats to schools. This guide helps you recognize and report them.

FVSD uses **KnowBe4** for security awareness training and the **Phish Alert Button** in Outlook for reporting suspicious emails. If you haven't completed your security awareness training, check your email for an invitation from KnowBe4.

What Is Phishing?

Phishing is when someone sends a fake email designed to trick you into:

- Clicking a malicious link
- Entering your password on a fake login page
- Downloading a harmful attachment
- Sharing personal or financial information

These emails often look like they come from a trusted source — Microsoft, Google, a colleague, or even your principal.

How to Spot a Phishing Email

Watch for these warning signs:

Suspicious Sender

- The email address doesn't match who it claims to be (e.g., an email "from Microsoft" sent from `support@m1cr0soft-alerts.com`)
- A colleague's name but a different or external email address

Urgency and Pressure

- "Your account will be locked in 24 hours"
- "Immediate action required"
- "You must verify your identity now"

Unexpected Requests

- Asking you to click a link to "verify" your password or account
- Requesting gift cards, wire transfers, or personal information
- An unexpected attachment you weren't expecting

Poor Writing

- Spelling and grammar mistakes
- Generic greetings like "Dear User" instead of your name
- Awkward phrasing or formatting

Suspicious Links

- Hover over links (don't click) — does the URL match where it claims to go?
- Look for misspelled domain names (e.g., `fvsd-login.com` instead of `fvsd.ab.ca`)

Real Examples From FVSD

Phishing emails targeting students and staff have included:

- Fake **job offers** sent to student email addresses — "You've been approved for an online part-time position" with no interview required
- Messages pretending to be from IT asking staff to "verify your email account"
- Fake shared documents — "Someone shared a file with you" with a link to a fake login page

What to Do If You Receive a Suspicious Email

1. **Do not click** any links or download any attachments

2. **Do not reply** to the email
3. **Report it** using the **Phish Alert Button** in Outlook:
4. Click the **Phish Alert** button in the Outlook toolbar
5. This sends the email directly to IT for review and removes it from your inbox automatically
6. If you don't see the Phish Alert button, contact IT to have it enabled

What to Do If You Clicked a Link or Entered Your Password

Don't panic — act quickly:

1. **Change your password immediately** (see the [Password Reset](#) article)
2. **Contact IT right away** — email helpdesk@fvsd.ab.ca
3. Let IT know exactly what happened — what you clicked, what information you entered

The sooner you report it, the faster IT can secure your account and prevent further damage.

Tips to Stay Safe

- **Never enter your FVSD password** on a page you reached by clicking an email link — instead, go directly to the site by typing the address yourself
- **Be skeptical of urgency** — legitimate services rarely threaten immediate account lockout
- **When in doubt, ask IT** — it's always better to check than to click
- **Talk to your students** — if you receive a suspicious email, your students may have received it too

Contact IT

- **Submit a ticket** through the IT helpdesk
- **Email:** helpdesk@fvsd.ab.ca

Revision #1

Created 2026-08-06 22:44:01 UTC by Admin

Updated 2026-08-06 22:44:01 UTC by Admin