GRADE·A

Cybersecurity Checklist

PHISHING

In our current digital landscape, it's critical to double-check all digital messages and files that you receive to ensure that the message is from a legitimate source. If a message seems slightly off, includes unusual grammatical mistakes, mysterious links, or unexpected information, it could be a scam.

- ☐ Does the email ask for your personal information?
- ☐ Check the sender's email address.
- ☐ Is the greeting personal?
- ☐ Is there poor spelling and grammar in the email?
- ☐ Does the signature look legitimate and have contact information?
- ☐ Is the attachment necessary?
- ☐ Does the attachment end in .exe?
- ☐ Hover over all links to make sure they will lead you to the right place.
- ☐ Are there any clear signs of common phishing tactics?
- ☐ Are there any other signs that this is a fake email? Do you feel it is suspicious? If so, report it or contact the company directly.

Additional Resources

For additional training resources and helpful links, visit **www.gradea.ca/securityresources**