THE OTTAWA GUILD OF POTTERS
LA GUILDE DES POTIERS D'OTTAWA

Good Email Habits to Prevent Fraud

- Check the sender's actual email address. Don't rely on the displayed name. A scammer can make an email appear to be from the president, treasurer, or the guild.
- Be suspicious of unexpected payment requests.
- Watch for a sense of urgency and pressure. Phrases like "pay immediately," "confidential," or "don't call me" are warning signs.
- Don't automatically click links. Hover over links and check where they actually lead. When in doubt, go to the company's website yourself and type in the URL path rather than using the link within the email.
- Check attachments carefully. Unexpected invoices or documents can contain malware or lead to fake login pages. In most cases, do not open attachments unless you have requested it.
- Look for unusual language or formatting. Spelling mistakes aren't proof of a scam, but unusual wording, formatting, or a sudden change in someone's writing style can be a clue.
- Don't assume internal emails are safe. A legitimate account can be compromised, so you should always verify an email from a familiar person if money is involved.
- Never provide passwords or security codes by email.
- When in doubt, stop. It's much easier to delay a payment for five minutes and verify it than to recover money after a fraudulent transfer.

A useful rule to remember

STOP → CHECK → VERIFY → PAY

STOP: Don't act because the email says it's urgent.

CHECK: Examine the sender, links, request, and attachments.

VERIFY: Contact the person/company independently.

PAY: Only proceed once the request is confirmed.