# Email scams and safety

Scammers and cybercriminals use the Internet, emails and spam to send out scams to millions of recipients.

**Please note:** legitimate organizations will not request personal, sensitive, confidential or financial information via an email. Use common sense when you're on the Internet and be careful about revealing personal information, such as your physical address, to anyone you meet in cyberspace, even if they claim to be someone of authority. This is called Phishing.

## Reporting email scams

If you've been targeted by an email scam or have identified one, please report it to the Canadian Anti-Fraud Centre. These may also be reported to the targeted website i.e. a bank or auction site. Scams that breach consumer protection laws may also breach the fraud provisions of the Canadian Criminal Code.

**Have you**:

- Been a victim of fraud
- Suffered a loss because of someone's dishonesty or deception
- Had property stolen
- Been threatened or assaulted by a scammer

If so, please report this online crime to local police at the non-emergency number 403-266-1234. By reporting scams, the authorities may be able to warn others about the scam to minimize the chance of the scam spreading further. If you have sent money to a 4-1-9 scam, are a victim or identity theft or think someone has gained access to your banking or credit account, report this to your financial institution immediately.

## Preventing email scams

All email users should following these tips to prevent getting scammed via email:

- Never open attachments or click on links from unknown sources. They may contain malware or "viruses," which can damage your computer. Look at the sender, the time and date, the subject line and the body before opening the email. If it raises your suspicions, delete the message.
- Be suspicious of emails asking for your password or any other personal information. Legitimate organizations will not ask for this information. As a rule, never share your password with anyone.
- Keep in mind the even trusted sources get their accounts hacked - if something seems suspicious, don't click on the link.

- Use an anti-virus program, firewall, spam blocker and anti-spyware technology. Keep all software and your operating system regularly updated to ensure they continue to protect as new technologies evolve.
- Learn to recognize spam and delete unsolicited messages immediately. Don't respond - responding confirms that you are a person with an active e-mail address.
- Always log out of your email when finished your work or whenever you have to leave your computer unattended.
- Do not send sensitive photographs, personal, financial or confidential information via email or in an instant message (IM.)
- Use age and gender neutral names as an email address and do not give out any personal information such as your cell phone number or address to anyone via email. Check your email signature for personal information.
- When sending emails to multiple recipients, place these personal email addresses in the blind carbon copy (Bcc) area. This helps to prevent exposing email addresses to others.
- Be aware of your family's email and IM activities. Children should expect that parents will view their online activities to make sure they are safe.
- Report unsolicited, harassing or offensive email to the Internet Service Provider or the customer service department of the source's e-mail.
- Be suspicious of emails that are overtly urgent sounding, frightening, official looking, congratulatory or secretive. Often times these kinds of emails entice the recipient to read the contents as an opening to communicate further with the sender.

# Common email scams

Nigerian Letter Scams (4-19 fraud), also referred to as "advance fee fraud," involves scammers asking for help with a transfer of money overseas. They often claim to be from a lawyer or bank representative advising of a huge inheritance.

Do not receive or cash any payments by cheque or money-order. The amounts are usually an overpayment and the scammer asks for a refund of funds before the victim discovers the cheque or money order has bounced. Furthermore, never send money or give credit card or online account details to anyone you do not know or trust.

Other popular email scams involve lotteries, contests, pyramid schemes, money transfer requests, dating scams, employment scams or health and medical scares.