Ontario Provincial Police
Police provinciale de l'Ontario

News Release/ Communiqué

FROM/DE: Corporate Communications **DATE: October 21, 2016**

VIRUSES, WORMS AND TROJANS – OH MY!
Attachments Contain Threats to Personal and Business Data Systems

(ORILLIA, ON) – Ontario Provincial Police (OPP) warn of the dangers presented by emails and certain attachments as part of its ongoing *Cyber Security Awareness Month* campaign.

Reading the contents of an email should be safe if you have the latest security patches, but email attachments can be harmful. Email phishing scams can trick you into opening attachments or giving up personal information. They appear to be emails from people, organizations or companies you know or trust, but they're often the gateway to identity theft by automatically installing malware, viruses, worms, and trojans. In some instances, email attachments are disguised as letters of reference, resumes or information requests can infiltrate and affect businesses that are involved in legitimate hiring processes. Also known as "spearphishing campaigns", high-value corporate and governments have been targeted through email attachments to take advantage of previously-unknown security vulnerabilities.

Many email servers will perform virus scanning and remove potentially dangerous attachments, but you can't rely on this. The easiest way to identify whether a file is dangerous is by its file extension, which tells you the type of file it is. For example, a file with the ".exe" file extension is a Windows program and should not be opened. Many email services will block such attachments. Other file extensions that can run potentially harmful code include ".msi", ".bat", ".com", ".cmd", ".hta", ".scr", ".pif", ".reg", ".js", ".vbs", ".wsf", ".cpl", ".jar" and more.

In general, you should only open files with commonly-used attachments that you know are safe. For example, ".jpg" and ".png" are image files and should be safe. Document files extensions such as ".pdf", ".docx", ".xlsx", and ".pptx" and should also be safe — although it's important to have the latest security patches so malicious types of these files can't infect systems via security holes in Adobe Reader or Microsoft Office.

If you or a business suspects they've been a victim of 'spearfishing', contact your local police service, the Canadian Anti-Fraud Centre, report it to the OPP online at http://www.opp.ca/index.php?id=132 or through Crime Stoppers at 1-800-222-8477 (TIPS) at https://www.tipsubmit.com/start.htm

For helpful tips and links during Cyber Security Awareness Month, follow the OPP on Twitter (@OPP_News), Facebook and Instagram and using the hashtags **#CyberSecurity**, **#CyberAware** and **#OPPTips**.

QUOTES

"Insecure, infected or unencrypted email attachments can risk injecting a number of information and data security threats to your home or workplace environments. Your personal information and business systems need to be safeguarded and it starts right at your inbox."

–Deputy Commissioner Rick BARNUM, OPP Investigations and Organized Crime

"When it comes to email attachments, you should exercise extreme caution and assume the worst. Don't actually download or run an attachment unless you have a good reason to do so. If you're not expecting an attachment, treat it with healthy suspicion."

– Supt. Paul BEESLEY, Director – OPP Behavioural, Forensic and Electronic Services

LEARN MORE

Email Risks (courtesy of Public Safety Canada)

Spearphishing: The Risk to Corporate Canada (courtesy of Public Safety Canada)

Get Cyber Safe Guide for Small and Medium Businesses (courtesy of Public Safety Canada)

Get Cyber Safe is a national, multi-jurisdiction, public awareness campaign created to educate Canadians about Internet security and the simple steps they can take to protect themselves online. Visit http://www.getcybersafe.gc.ca/

-30-

MEDIA NOTE: This is the fourth in a series of topic-specific OPP media releases to enhance community safety and awareness as part of international *Cyber Security Awareness Month*.

Media Contact: **Sgt. Peter LEON**
Provincial Media Coordinator

Phone: **705-329-6878**