Endura Manufacturing Co. Ltd
12425 149 Street
Edmonton, Alberta T5L 2J6
Toll Free: 1-800-661-9930
www.endurapaint.com

Cybersecurity Memo

To all Endura customers:

Re: Phishing and other email scams.
April 07, 2022

It has come to our attention that at several Endura customer have received a fraudulent email, that looks like it was sent by Endura, demanding payment for an overdue invoice.

The email address used by the sender was from the domain ”@endurapaint.com”.
This is a spoofed email address. Endura does not use endurapaint.com for email. All email communication from Endura will be from a @endura.ca address.

Endura Paint is committed to keeping your information safe and secure. Phishing is the most common tactic employed by hackers and we are taking additional steps to minimize phishing scams related to Endura Paint.

We will never send you unsolicited emails or text messages regarding:

1. Confidential information, such as your credit card number or other banking data.
2. Changes to payment terms, or accounts payable bank deposit change requests.
3. Demands for payment or requests to make payments in nonstandard currencies (Bitcoin, gift cards, etc.).

If you receive an unusual invoice, late payment notice or other communication from our accounting department, please contact us by phone. **If you receive any unexpected or unusual request for funds or data, ALWAYS check with our Accounts Payable department before sending money or confidential information.**

Additional email best practices to follow:

1. Do not open or click on any links or attachments from a person or senders that you do not recognize.
2. Be especially careful with .zip or executable file types (.exe).
3. NEVER provide sensitive personal information (credit card, banking info) through email. Emails are NOT a secure method for transferring financial information.)
4. If you are unsure if an email is legitimate or not, DO NOT open ANY attachments or click ANY links. Report the email to your IT department and verify its legitimacy.
5. You can also use online phishing tools to check your email security.
   One site is https://emailspooftest.com/ This page provides an automated email security risk assessment tool that can help assess your emails security configurations.
6. There are email configurations (DMARC, SPF etc) that can help to protect you from these spoofs, please talk to your IT provider to ensure your email security setting are properly setup.

Be especially cautious when opening attachments or clicking links if you receive an email containing a warning banner indicating that it originated from an external source outside your network.

If you think you’ve been targeted by a phishing or other scams, or notice something odd the next time you receive any emails or other communications from Endura Paint, please forward the original email to **helpdesk@endura.ca and call us at 1-800-661-9930 or 780-451-4242**

If you provided any information to the suspicious account, such as entering any banking or other secure information after clicking on a link, please immediately contact your bank or financial institution to report the situation and then email us at helpdesk@endura.ca and call us at 1-800-661-9930 or 780-451-4242