CITY OF PORTLAND

OFFICE OF MANAGEMENT AND FINANCE
BUREAU OF REVENUE AND FINANCIAL SERVICES
Ted Wheeler, Mayor
Michelle Kirby, Interim Chief Financial Officer
Thomas Lannom, Revenue Division Director

Tyler Wallace, Tax Division Manager
111 SW Columbia St., Suite 600
Portland, OR 97201-5840
Tel: (503) 823-5157
Fax: (503) 823-5192
TTY: (503) 823-6868

FOR IMMEDIATE RELEASE
Date: January 21, 2020

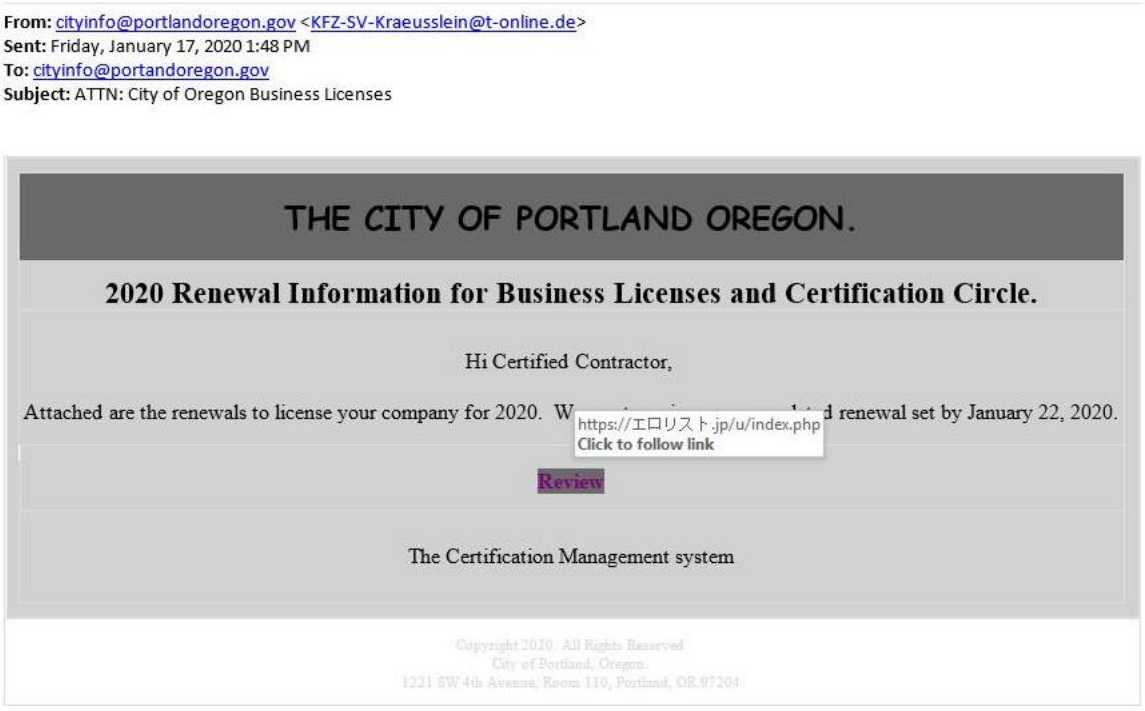
Contact: Heather Hafer, Public Information Officer
Office of Management and Finance
503-823-6965

Reminder to Taxpayers: Phishing and Security

The City of Portland Revenue Division has received several reports of business income taxpayers receiving phishing e-mails asking businesses to "renew… license[s] for your company for 2020." The request includes a link to "review" the renewal.

The City does not require taxpayers to renew business licenses, only to annually file a return.

A screenshot of a fraudulent request to "renew a license" is below.



From: cityinfo@portlandoregon.gov <KFZ-SV-Kraeusslein@t-online.de>
Sent: Friday, January 17, 2020 1:48 PM
To: cityinfo@portandoregon.gov
Subject: ATTN: City of Oregon Business Licenses

THE CITY OF PORTLAND OREGON.

2020 Renewal Information for Business Licenses and Certification Circle.

Hi Certified Contractor,

Attached are the renewals to license your company for 2020. W d renewal set by January 22, 2020.

https://エロリスト.jp/u/index.php
Click to follow link

Review

The Certification Management system

Below you will find the City of Portland's Bureau of Technology Services – Information Security Phishing Best Practices (Guidance).

Phishing is an email attack that appears to be from a reputable company and induces an individual to reveal personal information such as passwords or account information.

Phishing attacks are increasing in scope and sophistication. They also are getting harder to detect. There are three basic steps you can take and there are resources to help you better defend against phishing attacks and what you should do if you fall victim.

Identify and Detect Phishing:

- A phishing email tells a story intended to trick you into providing confidential information
- Often there is urgency or pressure to act quickly
- Requested information may be to confirm or complete personal details
- The requestor may appear to be a legitimate sender or pose as a trusted web address
- Use extra caution when emails contain links:
    - From a computer → Hover mouse (pointer) over the link (URL) to inspect the full link
    - From a smartphone → press the link – Don't tap – to reveal the full link
    - If the link looks long, has gibberish, or references a name you don't know and trust, do not click or tap on the link
- Do not open attachments that you are not expecting. Call the sender to confirm if you are unsure

Protect against Phishing:

- Make sure your device security and anti-malware software is up to date—and set to automatically update
- Protect your information and accounts with Multi-Factor Authentication (MFA)
- Protect your data by backing it up regularly and automatically

Recover from Phishing:

- If you have clicked or provided confidential information, report this to IdentityTheft.gov (https://www.identitytheft.gov/Info-Lost-or-Stolen) where you can identify the types of information lost or exposed. The federal government will not respond directly to you
- Report phishing attacks to ftc.gov/complaint and forward a copy of the email to reportphishing@apwg.org
- If the phishing attack was via text message, forward to SPAM (7726)
- Change your online and financial passwords, and add MFA to all accounts
- Notify your banking institutions, and request 'free credit freeze' from the major Credit Bureaus. You must reach out to the credit bureaus individually. Ask for the "FREE" freeze and un-freeze service. Here is a safe link to the FTC site for "How To": https://www.consumer.ftc.gov/blog/2018/09/free-credit-freezes-are-here
- Have your computer or device scanned for malware

An excellent, one-stop resource is the Federal Trade Commission phishing resource site: https://www.consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams.