BTS INFORMATION SECURITY NEWS

Phishing for Employees

In late June 2017 the Information Security Team at the City of Portland conducted a phishing exercise involving the entire City. This phishing campaign was conducted to see where the faults in employee's reactions to phishing is, and how effective our awareness training has been. A phish is an interaction with another person to gain personal information. This can be done in person, on the phone, or most likely an email. The goal of the email is to persuade an individual into clicking or downloading something that can harm their device and steal important information. Malware that locks devices out from the users and demanding payment to regain access can also be downloaded from this.

STOP | THINK | CONNECT™

A large majority of employees had reported the phishing email to the Helpdesk and information security. However, some did so after clicking the link. Follow the Stop, Think, Connect methods to reduce possibilities of an incident. Always Stop for a moment to Think about where you are going before you Connect to something.

- **Stop** - Take a moment to...
- **Think** - About your actions before you...
- **Connect** - To an unknown resource

Some employees did the right thing contacting the Helpdesk for assistance with the phishing email. Below is the sample email that was sent out.

Due to recent legal compliance issues, Microsoft is changing all email user's mailboxes to delete all messages over 45 days. To opt-out or adjust this setting, please follow the Microsoft provided instructions: please go to this link.

This setting will take effect on at the beginning of July.

Thank you,
Rick Astley
IT Service Desk

Phishing email sent to the City

What went well and not so well:

Q: Did employees report the phish?

A: Yes, but not all did so until after clicking the link. This means infection of your device would have already happen.

Q: Did employees avoid the phish?

A: A huge amount of employees did not open the email, or click the link. This implies that awareness training has been effective for some.

When at home

Take the lessons learned from this exercise and apply them to the way you deal with emails at home. Look for tall tale signs that the email is a phish. Poor grammar, and links to questionable websites are some of the things to look out for.

In some emails they will try to scare or excite you into clicking the link. Fear of some consequence or the excitement of a reward helps lower a persons judgement in clicking a link. Take the time to think before you connect.

Contact Us

For questions, concerns, or feedback regarding City information security please contact BTS InfoSec at: btsinfosec@portlandoregon.gov.

For all other BTS questions, please contact the BTS Help Desk: btshelpdesk@portlandoregon.gov. x35199