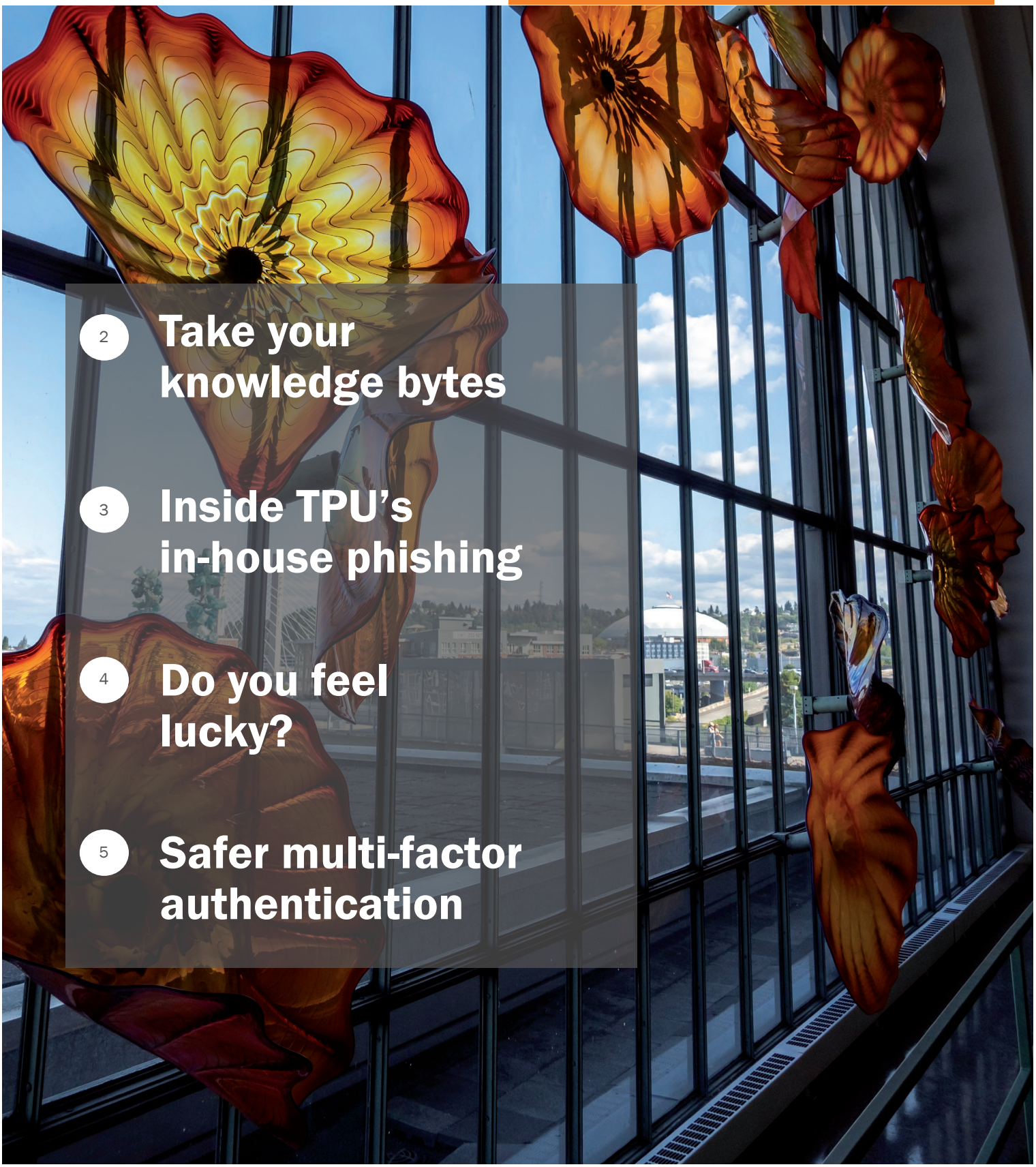
cybersecurity newsletter published by Tacoma Power

May 2022

security buzz



Take your knowledge bytes

Keep your cybersecurity skills in tip-top health. Engage in cyber fitness by taking a mini-course every month. The following optional trainings are yours to enjoy through June.

- **Fake News (S-162-FN-01)**
  (2 minutes)

False information has become part of our daily reality. View strategies for keeping fake news in check.

- **Home Cybersecurity (S-162-HS-01)**
  (1 minute)

Learn about steps to isolate, update, and defend to protect your home internet services and devices.

- **Incident Reporting (S-161-IR-01)**
  (7 minutes)

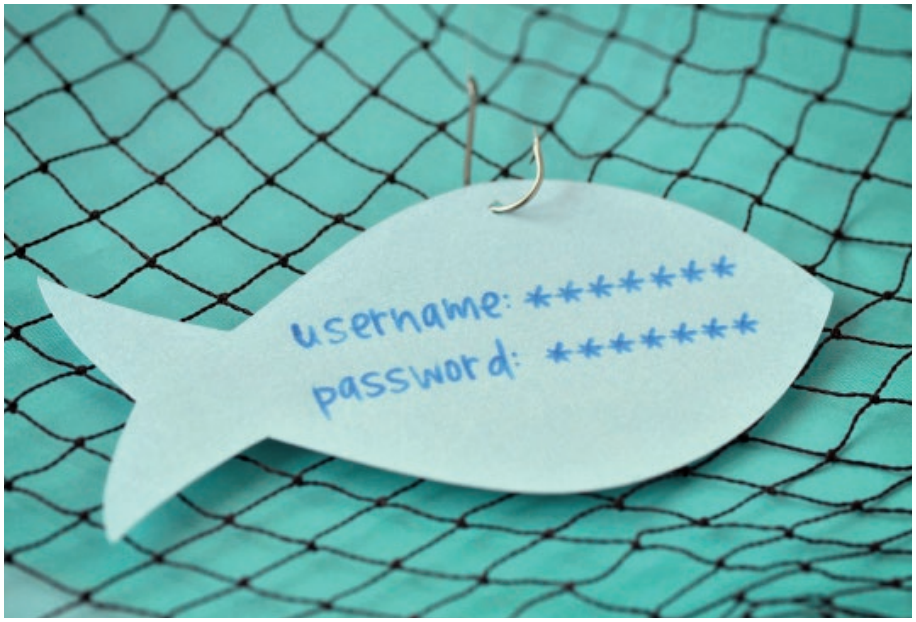
Learn about common physical and information security incidents you should report and why.

Here is how to login if you are logged into the City of Tacoma network:

1. Click on the learning portal link:
   https://learning.cityoftacoma.org.
2. Click My Courses
3. Locate <Course Name>.
4. Click on Launch Course.

If you are not logged into the City of Tacoma network, or if you are in a system other than the City of Tacoma network, exit from it. The following link requires access to an internet connection.

1. Click on the learning portal link:
   https://learning.cityoftacoma.org.
2. Enter your City of Tacoma network user name and password.
3. Click My Courses.
4. Locate <Course Name>.
5. Click on Launch Course.



Inside TPU's in-house phishing

Do you want to know what internal phishing results tell us about TPU's vulnerability? About which departments are most vulnerable? Why internal phishing emails are designed the way they are? What TPU's war on cybersecurity threats is trying to achieve?

- Learn why TPU phishing results are getting worse
- Learn clues that tell you an email is suspicious
- Learn the 2-second method for identifying a suspicious email

Come to learn the answers to these questions and to ask your own.

Add this date in your calendar:

Wednesday, Jun. 22, 2022 from 11:00 to 11:45 a.m.

Here is the Zoom meeting link to the live interactive session: https://us02web.zoom.us/j/81372909921.

Add the meeting to your Outlook calendar by downloading the iCalendar file here.

Mark your calendar for these additional meetings address the following topics:

- **Wednesday, Jul. 20** —Current phishing scams, protection guidelines from the FBI, and why electronic protections need the additional layer of employee recognition
- **Thursday, Aug. 18**—Seasonal online scams for you and your family to watch for

Questions may be directed to Rives Hassell-Corbiell at RHassellCorb@cityoftacoma.org.

Do you feel lucky?

Brute force is a hacking method. It uses trial and error to crack passwords to login credentials and encryption keys. Cracking is a method of identifying passwords by guessing all possible combinations of numbers and characters. It is costly, so it is not widely used, but it has a volume impact, extracting billions of passwords.

How quickly can passwords be cracked?

- Six characters takes 8 seconds.
- Seven takes less than 13 seconds.
- Eight takes 20 hours.
- Nine takes 80 days.
- 10 takes 21 years.

Feeling safe with a 12+-digit password? Just wait, there's more. Organized criminals and governments, or anyone who can afford to spend $20,000 on equipment, can crack up to 100 billion encrypted (with SHA256) passwords per second. Professional bad guys can buy databases of leaked passwords, millions at a time.

Using breached usernames and password pairs, automated systems probe more than 20 million accounts daily, inserting breached credentials into website login forms to fraudlently gain access to user accounts, such as bank accounts, medical accounts, and Amazon. Because more than 65% of users admit to reusing a password, more than one account per password can be compromised.

Don't be victim. Evaluate your passwords.

- Is your password likely to be unique in all the world? A nonsense phrase with punctuation, upper and lower case letters, and numbers might fit the bill.
- Is it at least 12 characters in length? From 12-15 characters is the current minimum best practice.
- Does it exclude names (including pets), dates, headlines, TV, movie or book titles, or popular phrases? Lists with all that information can be purchased.
- Is it a pattern on the keyboard, such as across, diagonal, every other one, alternating numbers and letters or lower and upper case? Any pattern is vulnerable.
- Safer alternatives for creating passwords include using a password generator, or a muti-factor authentication (MFA) application, like the one you use to log into the City of Tacoma VPN.

Good friends, co-workers, and families don't let those they love be an 8-second statistic. Pass the word.

Source: https://techcommunity.microsoft.com/t5/azure-active-directory-identity/your-pa-word-doesn-t-matter/ba-p/731984

Safer multi-factor authentication

Secure multi-factor authentication is moving away from codes sent to your email or text message accounts due to their vulnerability to being compromised.

Authentication applications, like RapidIdentity, used to log into the City of Tacoma VPN, are now being recommended for better security.

For the highest level of security to date, plug-in authenticators like Yubico are considered the most secure.

Not all locations you visit may be able to provide these authentication options, but the more that do provide you with greater protection.

You might want to consider moving to one or both of these methods in all of your personal accounts.

Visit the internet to find out more about these applications and devices, their ratings, and reviews.