Strengthening Your Organization's First Line of Defense, the Humans

2024 BU Security Camp

Worcester Polytechnic Institute Presenters:

Julius Newton, Information Security Analyst

Sharon Robsky, Technical Communications Specialist

Kerrie Sacovitch, Assistant Director, Communication & Change Management

We love your pet posts, but don't use their name in your password.

Agenda

- About the presenters
- Why cybersecurity awareness matters
- Where we started
- Changing it up!
- Partnerships & Resources
- Successes, Lessons Learned
- Next Steps: Continuous improvement & new initiatives

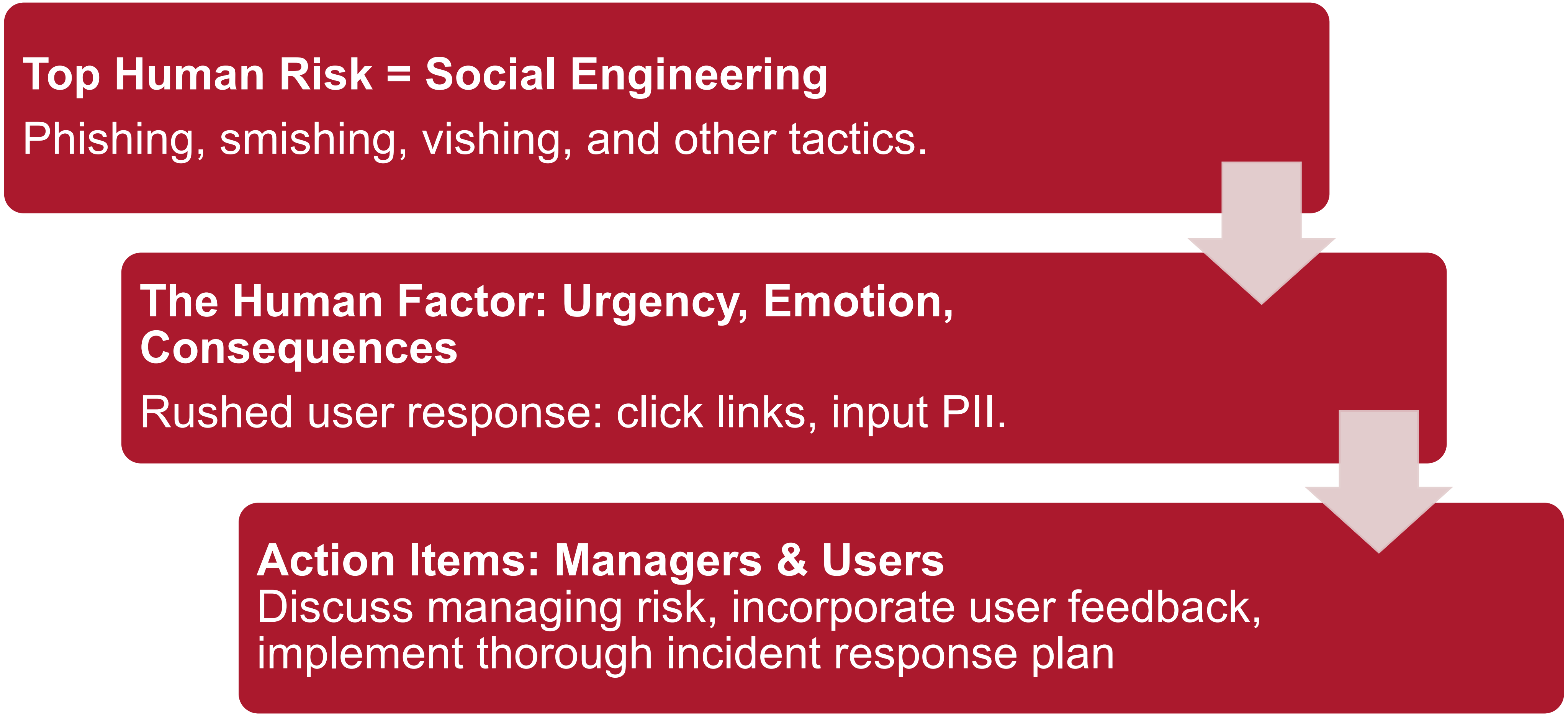
About the Presenters

- Julius Newton, Information Security Analyst
  - One thing most people do not know about me is I love to play chess.
  - Contact: jnewton@wpi.edu LinkedIn

- Sharon Robsky, Technical Communications Specialist
  - She's an avid knitter and recently finished 3 emotional support chickens.
  - Contact: srobsky@wpi.edu LinkedIn

- Kerrie Sacovitch, Assistant Director, Communication & Change Management
  - Made an AM radio commercial in first job as a teenager!
  - Contact: kls@wpi.edu WPI Profile LinkedIn

Why Cybersecurity Awareness Matters



Top Human Risk = Social Engineering

Phishing, smishing, vishing, and other tactics.

The Human Factor: Urgency, Emotion, Consequences

Rushed user response: click links, input PII.

Action Items: Managers & Users

Discuss managing risk, incorporate user feedback, implement thorough incident response plan

2023 SANS Institute Security Awareness Report Managing Human Risk

Benefits of a User Awareness Program

Users are an organization's first line of defense

Updates users on current trends, such as AI and deepfake

Provides guidance to victims

Reduces the risk of a data breach

Gain efficiency - less time spent on tickets, issues

Where We Started

Technology Orientation
for
New Employees

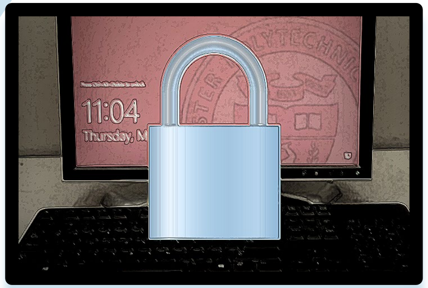
Orientations

Workshops

NCSAM

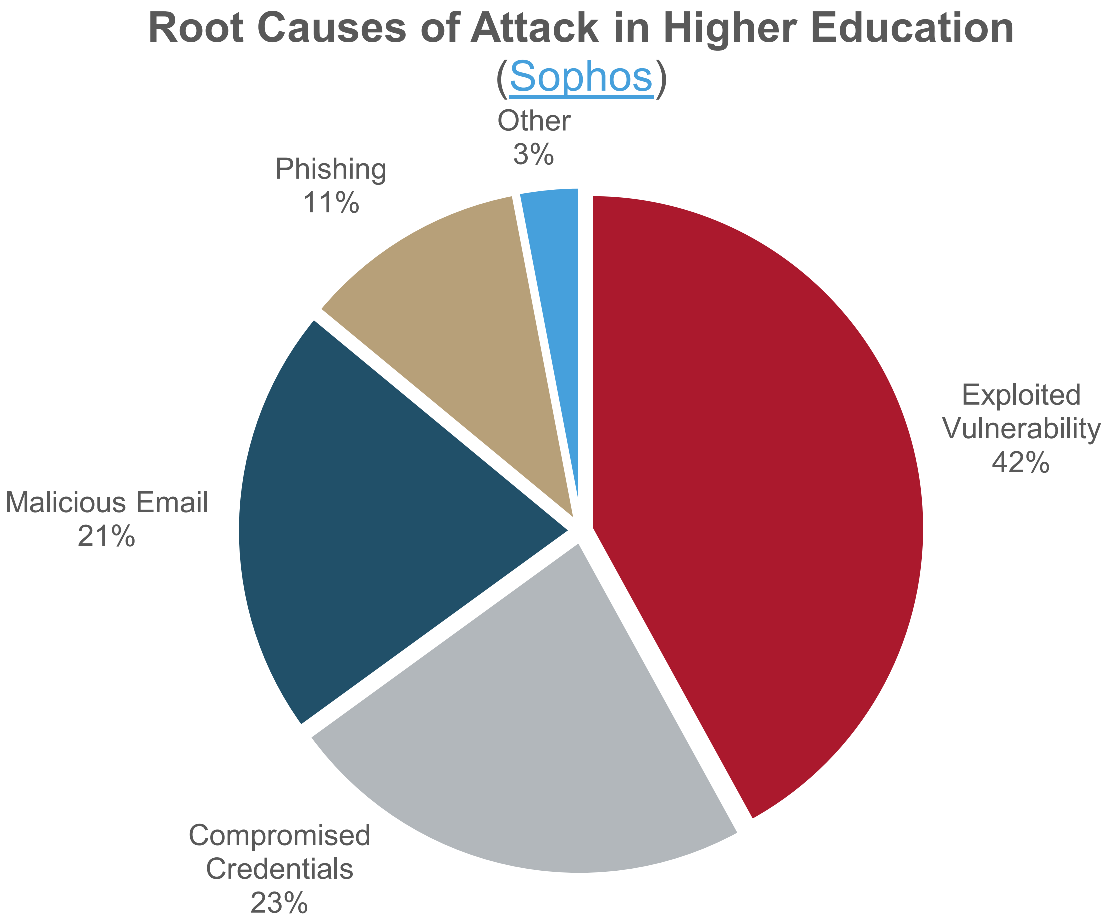
Compliance Training

Quarterly Newsletter



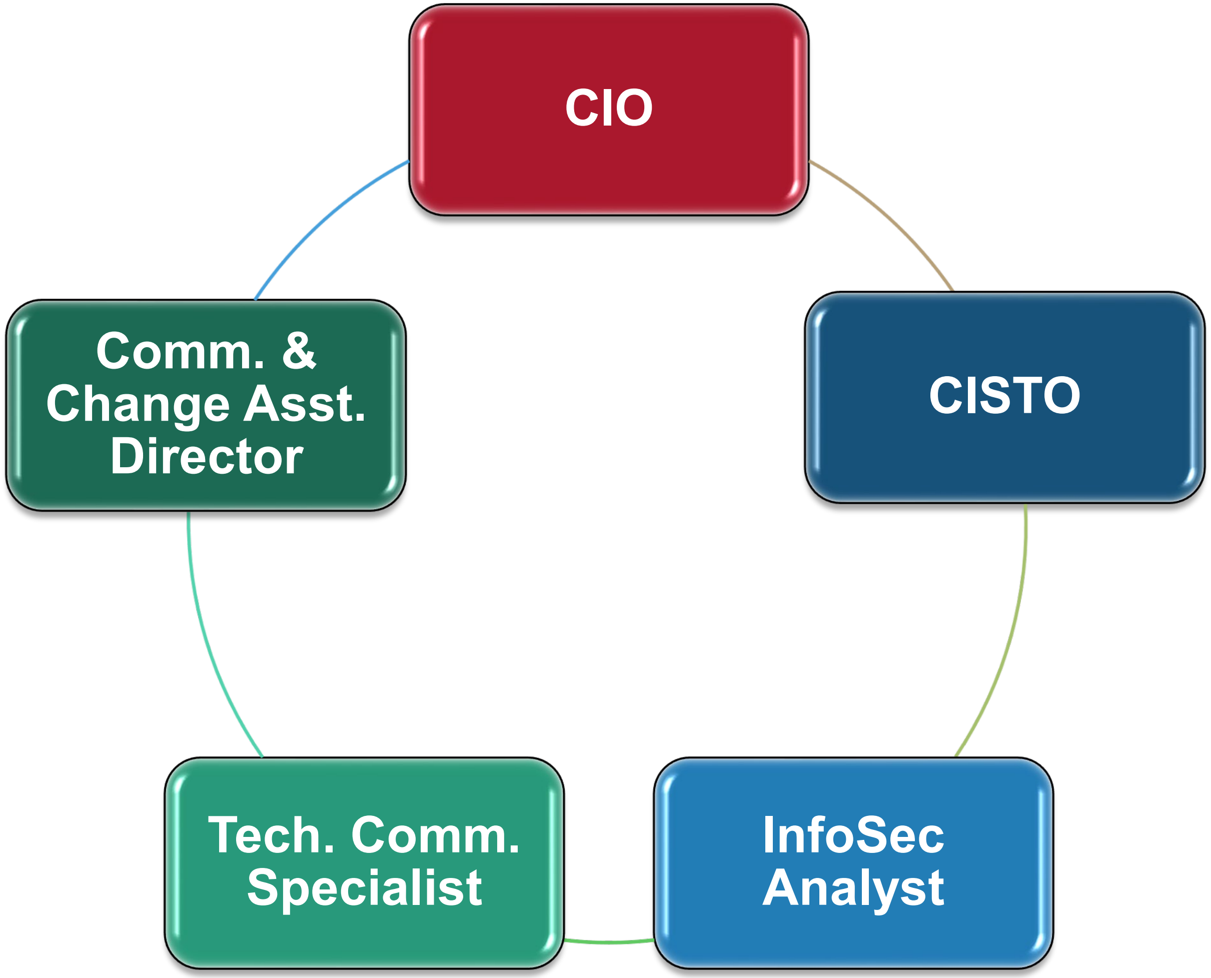
Why We Needed to Change

- Training not mandatory
- Increasing security challenges, higher ed breaches, advanced attack methods
- BOT security initiatives included education, Data Privacy Assessment
- Community buy-in for upcoming security process changes



The People!

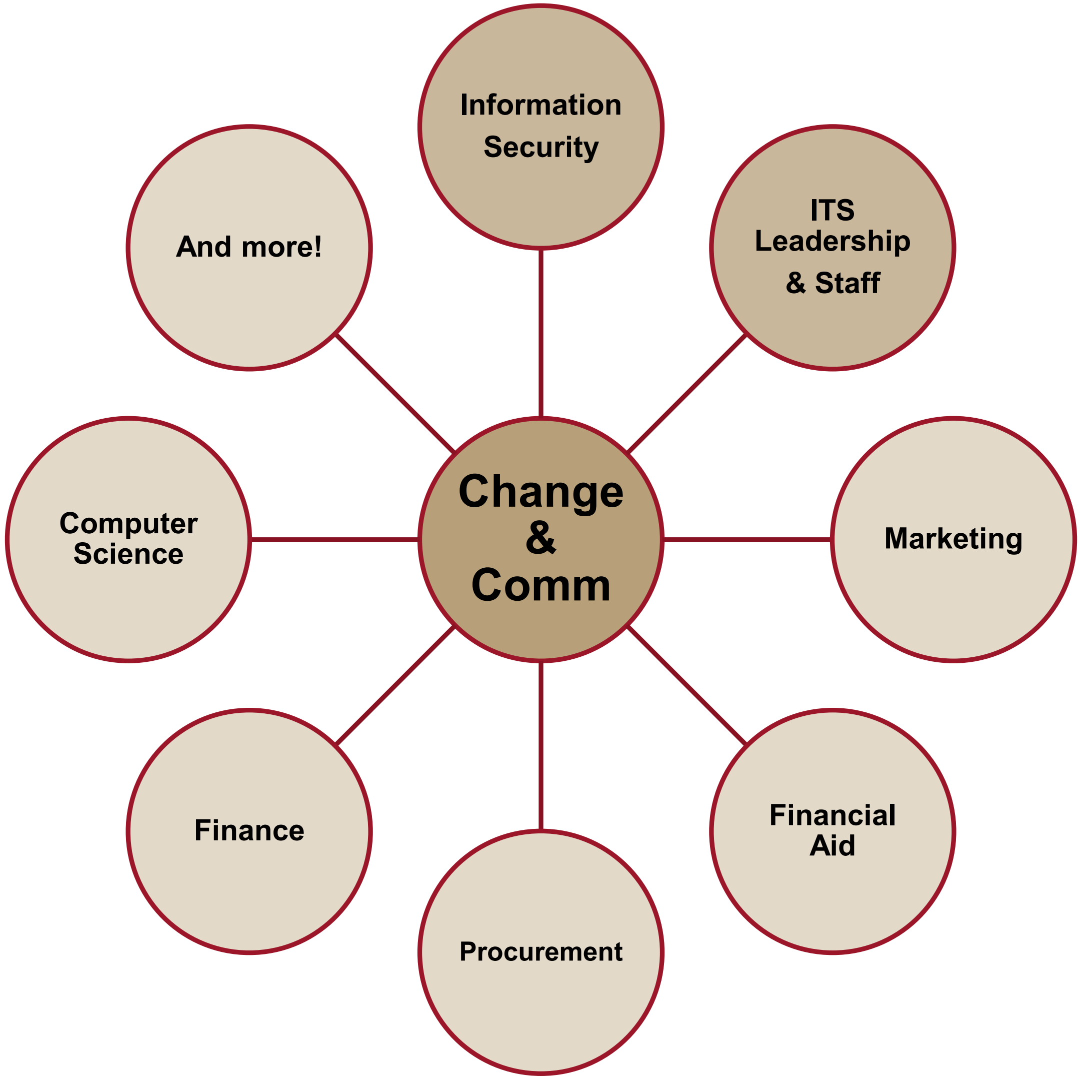
CIO & CISTO
Sponsorship


CIO
CISTO
InfoSec Analyst
Tech. Comm. Specialist
Comm. & Change Asst. Director

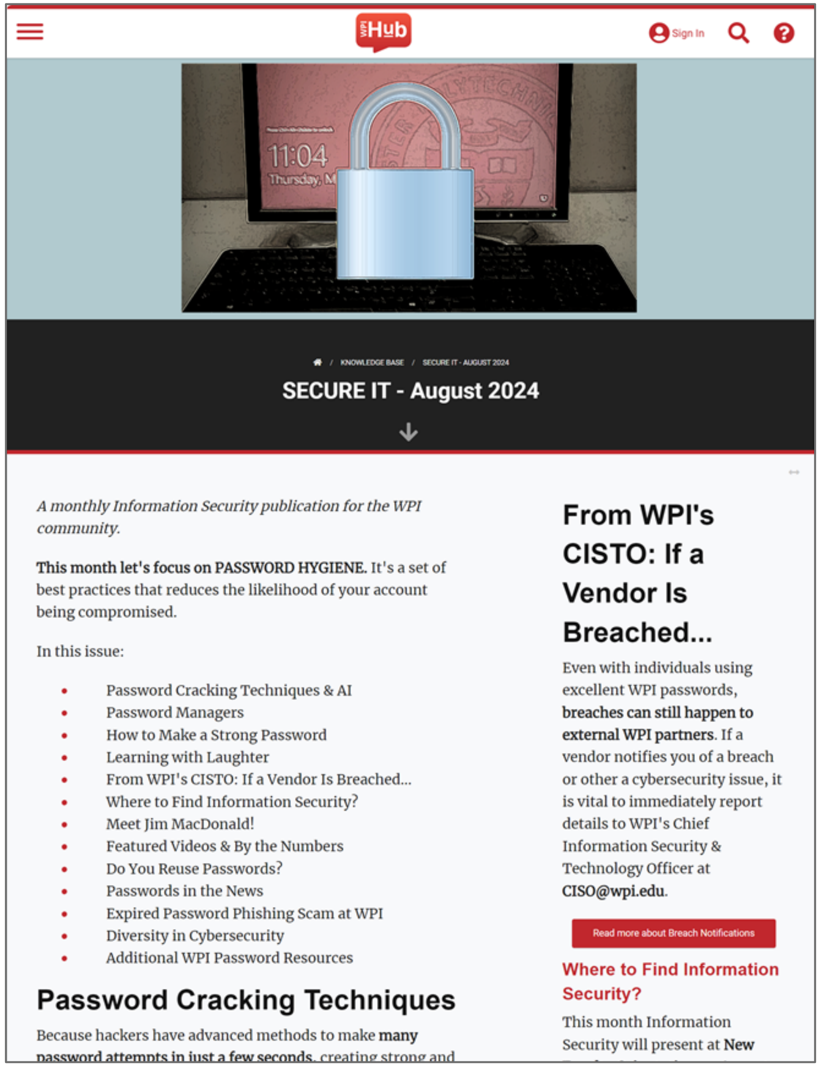
The Plan! 12 Month Map

- Academic/Administrative Annual Cycle
- Calendar Considerations
- Monthly Focus Topics
- Partnerships
- Outreach!

The Partnerships! Year #1



The Newsletter!



KNOWLEDGE BASE / SECURE IT - AUGUST 2024

SECURE IT - August 2024

A monthly Information Security publication for the WPI community.

This month let's focus on PASSWORD HYGIENE. It's a set of best practices that reduces the likelihood of your account being compromised.

In this issue:

- Password Cracking Techniques & AI
- Password Managers
- How to Make a Strong Password
- Learning with Laughter
- From WPI's CISTO: If a Vendor Is Breached...
- Where to Find Information Security?
- Meet Jim MacDonald!
- Featured Videos & By the Numbers
- Do You Reuse Passwords?
- Passwords in the News
- Expired Password Phishing Scam at WPI
- Diversity in Cybersecurity
- Additional WPI Password Resources

Password Cracking Techniques

Because hackers have advanced methods to make **many password attempts in just a few seconds**, creating strong and

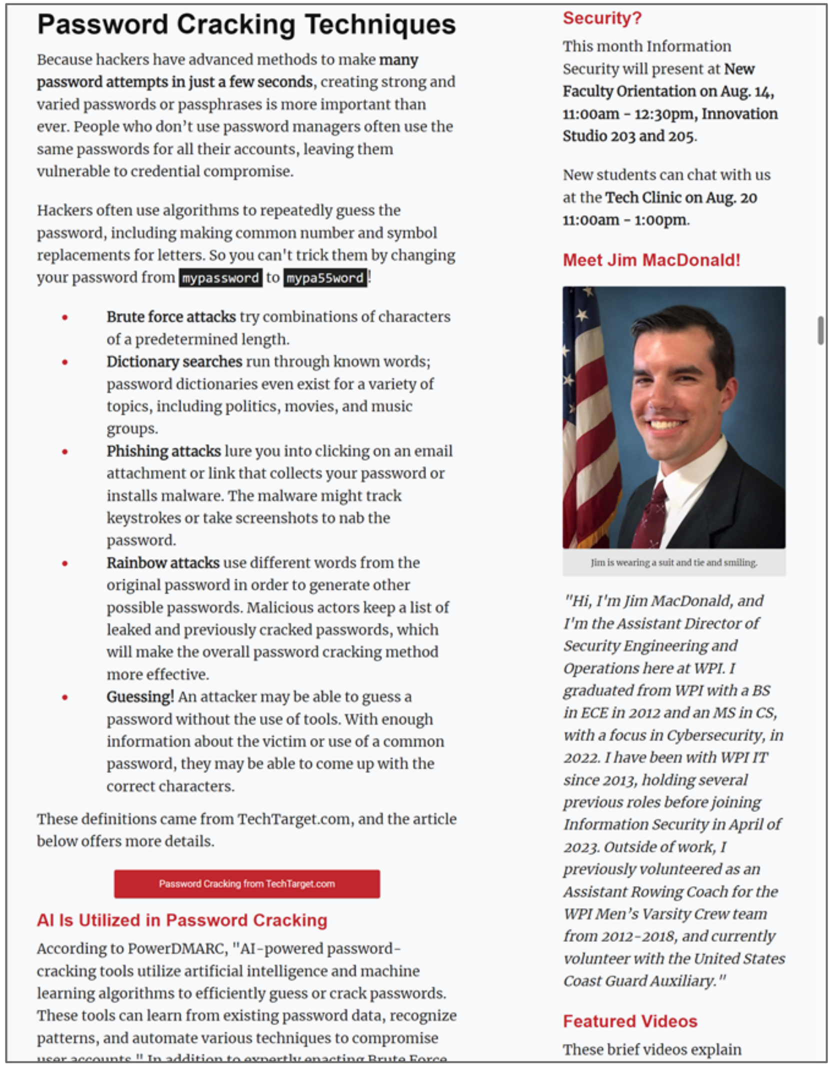
From WPI's CISTO: If a Vendor Is Breached...

Even with individuals using excellent WPI passwords, **breaches can still happen to external WPI partners**. If a vendor notifies you of a breach or other a cybersecurity issue, it is vital to immediately report details to WPI's Chief Information Security & Technology Officer at CISO@wpi.edu.

Read more about Breach Notifications

Where to Find Information Security?

This month Information Security will present at New



Password Cracking Techniques

Because hackers have advanced methods to make **many password attempts in just a few seconds**, creating strong and varied passwords or passphrases is more important than ever. People who don't use password managers often use the same passwords for all their accounts, leaving them vulnerable to credential compromise.

Hackers often use algorithms to repeatedly guess the password, including making common number and symbol replacements for letters. So you can't trick them by changing your password from `mypassword` to `mypa55word`!

- **Brute force attacks** try combinations of characters of a predetermined length.
- **Dictionary searches** run through known words; password dictionaries even exist for a variety of topics, including politics, movies, and music groups.
- **Phishing attacks** lure you into clicking on an email attachment or link that collects your password or installs malware. The malware might track keystrokes or take screenshots to nab the password.
- **Rainbow attacks** use different words from the original password in order to generate other possible passwords. Malicious actors keep a list of leaked and previously cracked passwords, which will make the overall password cracking method more effective.
- **Guessing!** An attacker may be able to guess a password without the use of tools. With enough information about the victim or use of a common password, they may be able to come up with the correct characters.

These definitions came from TechTarget.com, and the article below offers more details.

Password Cracking from TechTarget.com

AI Is Utilized in Password Cracking

According to PowerDMARC, "AI-powered password-cracking tools utilize artificial intelligence and machine learning algorithms to efficiently guess or crack passwords. These tools can learn from existing password data, recognize patterns, and automate various techniques to compromise user accounts." In addition to expertly enacting Brute Force

Where to Find Information Security?

This month Information Security will present at **New Faculty Orientation on Aug. 14, 11:00am – 12:30pm, Innovation Studio 203 and 205**.

New students can chat with us at the **Tech Clinic on Aug. 20 11:00am – 1:00pm**.

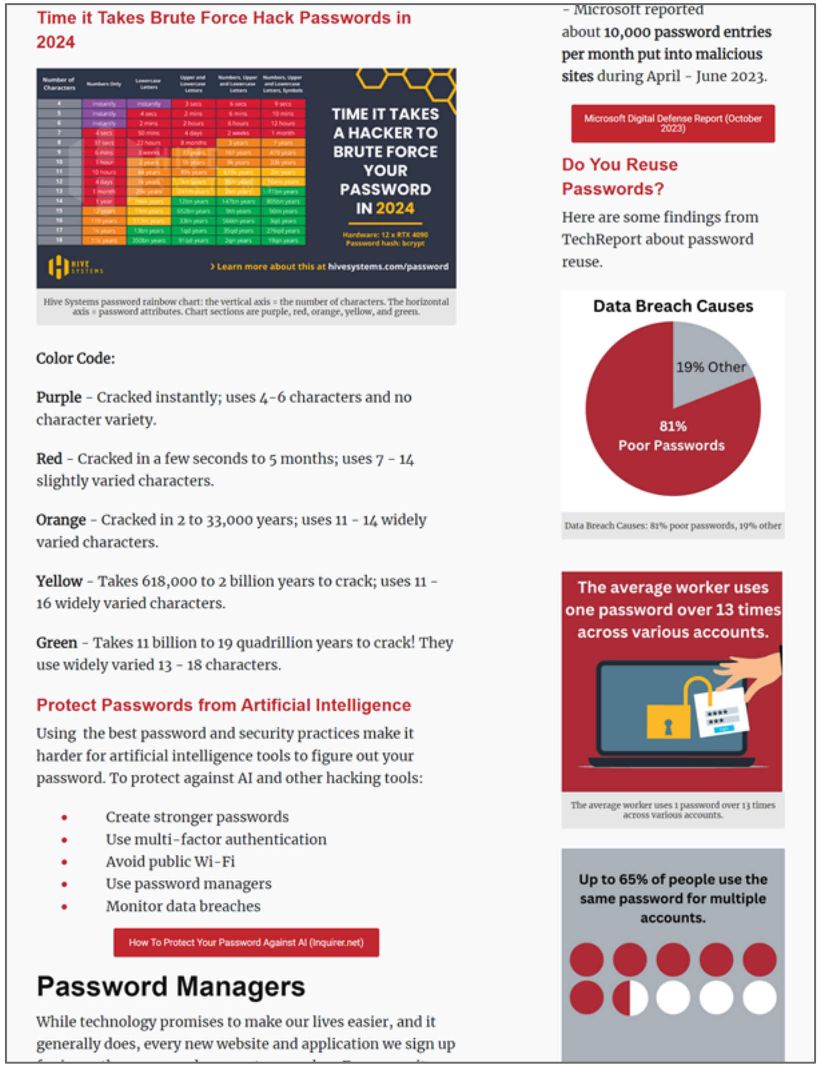
Meet Jim MacDonald!

Jim is wearing a suit and tie and smiling.

"Hi, I'm Jim MacDonald, and I'm the Assistant Director of Security Engineering and Operations here at WPI. I graduated from WPI with a BS in ECE in 2012 and an MS in CS, with a focus in Cybersecurity, in 2022. I have been with WPI IT since 2013, holding several previous roles before joining Information Security in April of 2023. Outside of work, I previously volunteered as an Assistant Rowing Coach for the WPI Men's Varsity Crew team from 2012–2018, and currently volunteer with the United States Coast Guard Auxiliary."

Featured Videos

These brief videos explain


TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD IN 2024
Hardware: 12 x RTX 4090
Password hash: bcrypt
Number of Characters
Numbers Only
Lowercase Letters
Upper and Lowercase Letters
Numbers, Upper and Lowercase Letters
Numbers, Upper and Lowercase Letters, Symbols
HIVE SYSTEMS
Learn more about this at hivesystems.com/password

Time it Takes Brute Force Hack Passwords in 2024

Hive Systems password rainbow chart: the vertical axis = the number of characters. The horizontal axis = password attributes. Chart sections are purple, red, orange, yellow, and green.

Color Code:

Purple – Cracked instantly; uses 4–6 characters and no character variety.

Red – Cracked in a few seconds to 5 months; uses 7 – 14 slightly varied characters.

Orange – Cracked in 2 to 33,000 years; uses 11 – 14 widely varied characters.

Yellow – Takes 618,000 to 2 billion years to crack; uses 11 – 16 widely varied characters.

Green – Takes 11 billion to 19 quadrillion years to crack! They use widely varied 13 – 18 characters.

Protect Passwords from Artificial Intelligence

Using the best password and security practices make it harder for artificial intelligence tools to figure out your password. To protect against AI and other hacking tools:

- Create stronger passwords
- Use multi-factor authentication
- Avoid public Wi-Fi
- Use password managers
- Monitor data breaches

How To Protect Your Password Against AI (Inquirer.net)

Password Managers

While technology promises to make our lives easier, and it generally does, every new website and application we sign up

– Microsoft reported about **10,000 password entries per month put into malicious sites** during April – June 2023.

Microsoft Digital Defense Report (October 2023)

Do You Reuse Passwords?

Here are some findings from TechReport about password reuse.

Data Breach Causes: 81% poor passwords, 19% other

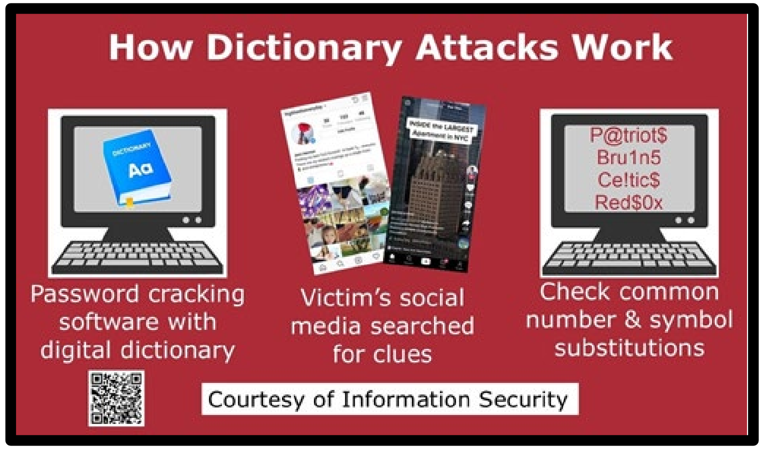
The average worker uses one password over 13 times across various accounts.

The average worker uses 1 password over 13 times across various accounts.

Up to 65% of people use the same password for multiple accounts.

Getting the Word Out

WPI Hub



How Dictionary Attacks Work

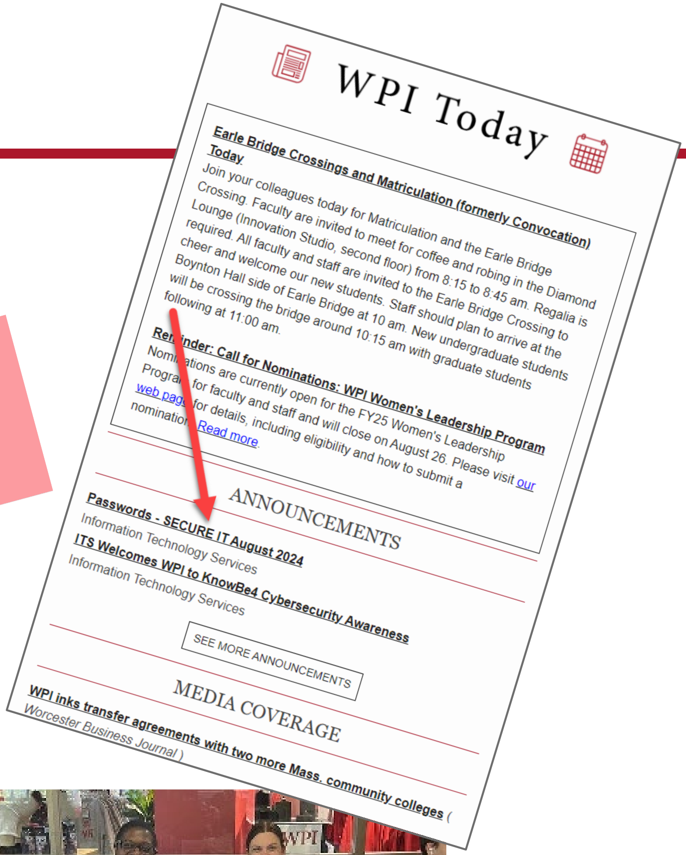
Password cracking software with digital dictionary

Victim's social media searched for clues

Check common number & symbol substitutions

Courtesy of Information Security

Instagram



WPI Today

Earle Bridge Crossings and Matriculation (formerly Convocation) Today
Join your colleagues today for Matriculation and the Earle Bridge Crossing. Faculty are invited to meet for coffee and robing in the Diamond Lounge (Innovation Studio, second floor) from 8:15 to 8:45 am. Regalia is required. All faculty and staff are invited to the Earle Bridge Crossing to cheer and welcome our new students. Staff should plan to arrive at the Boynton Hall side of Earle Bridge at 10 am. New undergraduate students will be crossing the bridge around 10:15 am with graduate students following at 11:00 am.

Reminder: Call for Nominations: WPI Women's Leadership Program
Nominations are currently open for the FY25 Women's Leadership Program for faculty and staff and will close on August 26. Please visit our web page for details, including eligibility and how to submit a nomination. Read more.

ANNOUNCEMENTS

Passwords - SECURE IT August 2024
Information Technology Services

ITS Welcomes WPI to KnowBe4 Cybersecurity Awareness
Information Technology Services

SEE MORE ANNOUNCEMENTS

MEDIA COVERAGE

WPI inks transfer agreements with two more Mass. community colleges (Worcester Business Journal)

Campus Announcements

Successes

- 12 newsletter issues published!
- Partnerships between IT and other departments
- Expanded Outreach: meet the team, webinars, table sitting
- Positive adoption of MFA and Alumni Email changes
- Cybersecurity Insurance: cost reduced + more coverage!

Lessons Learned

- Documentation: Teams channel, annual plan, publication checklist
- Schedule monthly meetings for planning, sponsor review
- General + WPI-specific = Widely Applicable
- Cross-campus collaboration – advance arrangements
- Photo Shoot to get noticed!
- Varied formats for varied audiences
- Groundwork for new initiatives
- Improve tracking

SECURE IT Continuous Improvement

- Update with timely info, links
- Revisit topics, incorporate new initiatives
- Email: variation, statistics
- Assess website for better tracking

See how we updated our Password Hygiene issue from year #1 to year #2!

SECURE IT – August 2023
SECURE IT – August 2024

Next Steps: Awareness Initiatives for 2024-2025

- KnowBe4 training and phishing simulations – with statistics!
- Monthly Instagram posts
- Student worker video collaboration

NEW!

Thank You for Attending!

- You are welcome to peruse issues by searching SECURE IT at hub.wpi.edu. Here are a few:

  October 2023: MFA

  February 2024: Tax Scams & Financial Aid

  May 2024: Summer Scams

- KnowBe4 Welcome Message
- Happy to share more - Contact us!

***Put simply,
hackers recognize that it is
easier to hack a human
than it is to hack a machine.***

Ruairi O'Donnellan, Intuition Blog

WORCESTER POLYTECHNIC INSTITUTE

LEHR UND KUNST

1865