The 3 P's of Cybersecurity

Quick Tips to Stay Safe

govloop

SECURELINK
THIRD-PARTY SECURITY

Introduction

PWK = Phone. Wallet. Keys.

Is there anything more frustrating than forgetting your phone, wallet or keys? Well, if you never want to leave behind these items again, just recite “PWK” while heading out the door.

Why isn’t there something like that for cybersecurity?

In these few, easy pages, we’ll give you just the thing. Ahead, you’ll explore activities, quizzes and easy tips for three main cybersecurity areas that are good at work or at home:

- **Passwords**
- **Physical Security**
- **Phishing**

For more information, download the full cybersecurity guide, which features even more, including a crossword puzzle!

PASSWORDS

What Makes a Good Password?

Maricopa County

- Passwords should be easy to remember, but hard to guess.
- Passwords should not be written down.
- Passwords should be at least eight characters long, containing mixed-case characters and special symbols or numbers.
- Passwords should not be easy-to-guess key sequences (e.g. “qwerty”).
- Passwords should not be dictionary words.

How long would it take for a high-powered server to guess these passwords?

- Today123 – 36.99 minutes
- Today1234! – 19.24 years
- Mi55ouriR!v3r – **1.65 hundred thousand centuries**

North Dakota

Our network and software security and firewalls can be the best and yet, if someone obtains our password, all the security in the world will not protect our data.

Do not include:

- Names
- Birthdates
- Seasons
- Hometowns
- Favorite team names, etc.

Hackers focus on the region of their potential victim, so they may try Fall2019, Vikings1, Packers1, Fargo2020, etc. as password attempts.

PASSWORDS

What to Do When There Are So Many

Password Manager: "Programs called password managers offer the option to create randomly generated passwords for all of your accounts. You then access those strong passwords with a master password."

– *Cybersecurity and Infrastructure Security Agency*

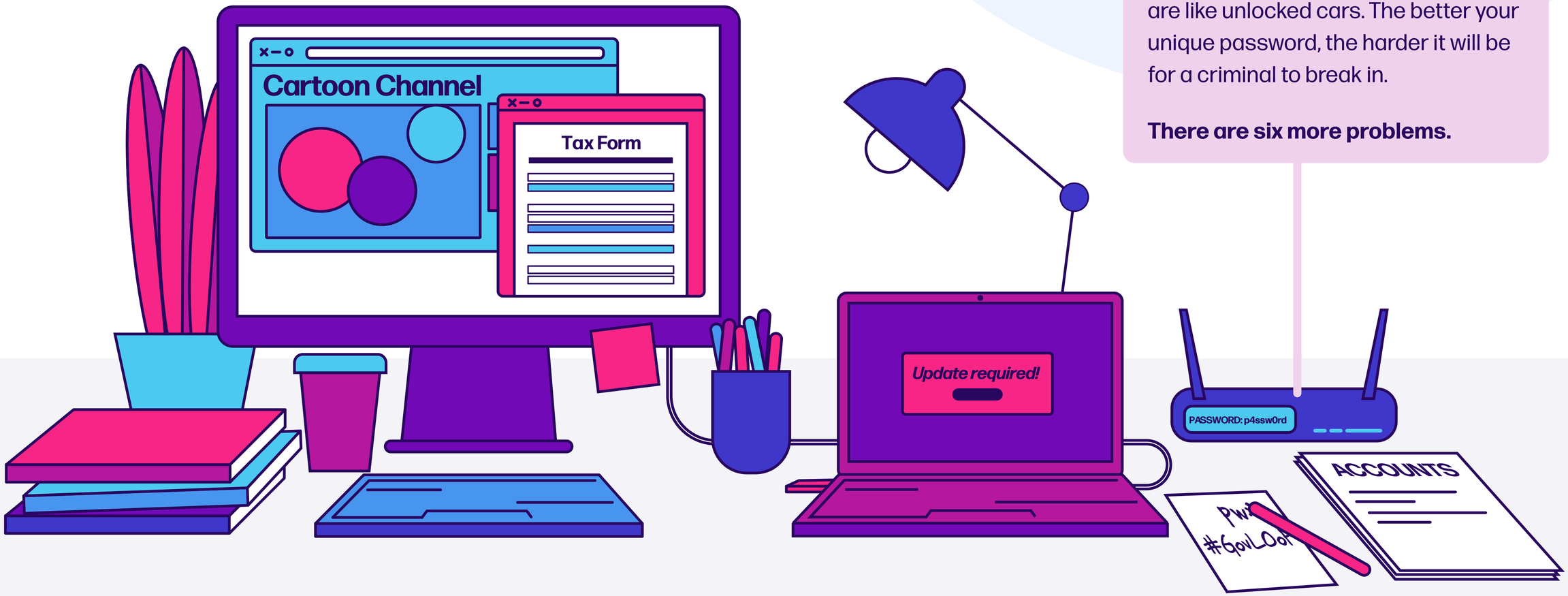
What should you look for when seeking a password manager solution?

- **Lock-In Period:** Can you easily switch your information to another product if you don't like the first one?
- **Multifactor Authentication (MFA):** Does it require users to provide at least two ways of identifying themselves, such as with a code provided in an email, text or voicemail in addition to a password or passcode?
- **Cross-Platform Capabilities:** Does it support each device platform you use?
- **Mobile Device Features:** What mobile device features does it have? For example, does it have biometric options instead of complicated passcodes?
- **Management:** Does it have a browser toolbar or menu to manage multiple saved accounts?
- **Autofill:** Will it autofill forms similar to your web browser?
- **Usability:** Is it easy to use?

PHYSICAL SECURITY

What's Wrong With This Image?

Play along with this activity. Identify security risks below, and check your answers on the next page.



Here's a freebie:
Change the default password on your home router. Cybercriminals are like car thieves, and default passwords are like unlocked cars. The better your unique password, the harder it will be for a criminal to break in.

There are six more problems.

PHYSICAL SECURITY

Cyberthreats Identified

Turn off your computer or put it in sleep mode while you're away from it.

Separate your work and home lives by creating different accounts or using different devices.

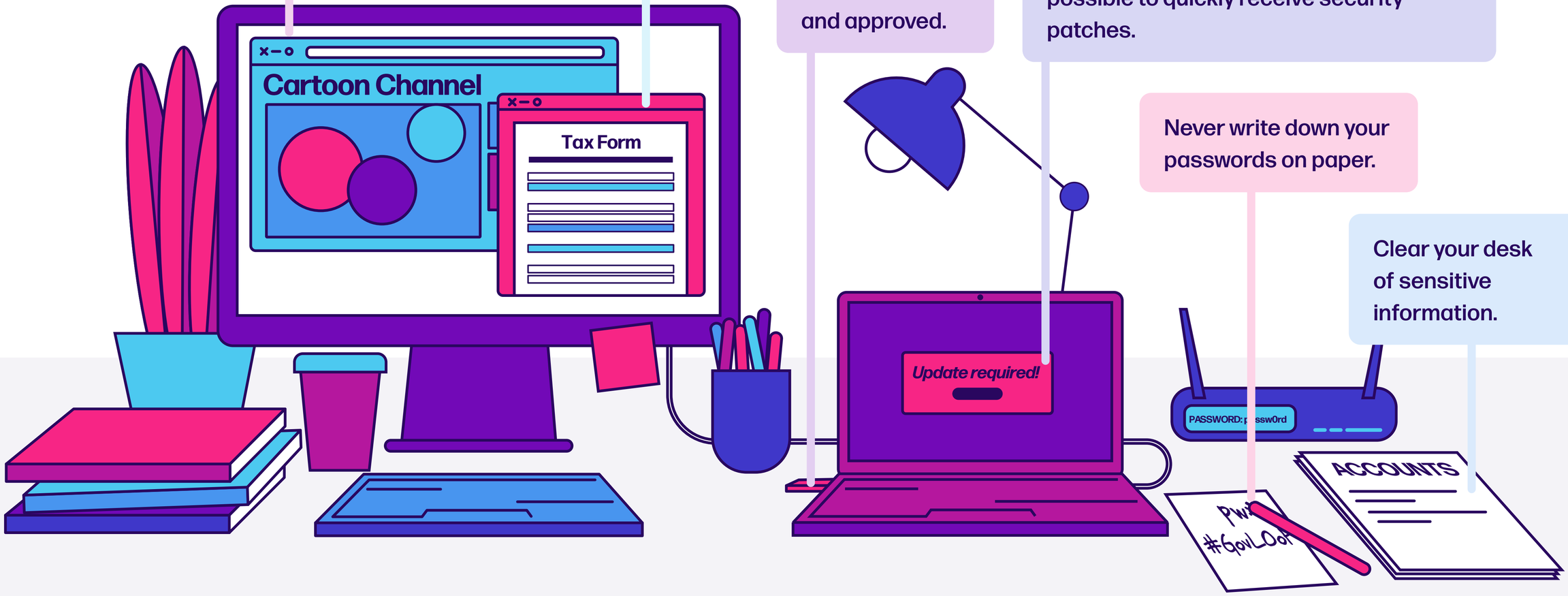
Double-check that external drives and plug-ins are secure and approved.

Update your computer as quickly as possible to quickly receive security patches.

Never write down your passwords on paper.

Clear your desk of sensitive information.

Don't forget: Watch out for webcams at home!



PHISHING

How to Catch a Phishing Attempt

Phish: A technique used by hackers to obtain sensitive information. An example is a hand-crafted email message designed to trick people into divulging personal or confidential data, such as passwords and bank account information.

This email seems a little phishy >>

From: cloudservicesteam45@gmail.com

Subject: Your Account Info

Hi Friend,

We've noticed some unrecognized activity going on on your Web Client account.

As a result, we've locked your account.

To open it up, you'll need to provide us with your account information and proof of identification. It's an easy process; just respond to this email.

– Your Cloud Services Provider

Sometimes, you can tell from the sender alone. Why would the official company have an odd address with numbers like this one?

Be wary of emails that target account information.

Notice the generic opening. That could be so they can send this email to lots of people.

Strange capitalizations and phrasings can be a dead giveaway.

Is your account actually locked? Close the email and go to the website you usually use to check.

This information is almost never solicited by email. Call the company at a known number to ask whether this was them.

PHISHING

Don’t Forget Checklist

What if you fell for a phishing attempt?

If they stole some of your information: Don’t panic, but act quickly. Go to IdentityTheft.gov if they have your information, and report the attempt to your IT department if it’s at work. Also, let the FBI know.

If they stole some of the agency’s information: Report it immediately to the IT team. Time is of the essence. Change the passwords for any personal accounts that you might have given them access to. If you’re able, encrypt information you’re sending over.

For suspicious communications...

NEVER:

- X **Respond with information**
- X **Click on links**
- X **Download attachments**
- X **Share with colleagues outside of IT**

ALWAYS:

- √ **Avoid any links or attachments**
- √ **Report to proper channel**
- √ **Inform others who may have been exposed**
- √ **Delete the email**

Virtual Meeting Tips & Tricks

Be mindful of your environment

Review your surroundings:

- Remove items with personally identifiable information (PII) from sight
- Keep in mind your camera view may change, so be aware of all your surroundings

Know of all laws that may be applicable

- Make sure that your public video meeting complies with any legal requirements
- Be cognizant of any sort of notification and instructions you wish to share with participants

Security is key!

To reduce the risk of disruptive elements:

If possible ...

- Require attendees to register for the meeting
- Require them to authenticate before attending
- Password-protect your meeting

If necessary, use a virtual background.

How to: *On Zoom or similar platforms, hit the arrow within the "Start Video" button. Select "Choose Virtual Background," and either pick a preselected image, or add your own!*

Industry Spotlight: SecureLink

The number of state and local government cyberattacks continues to rise. In 2020, at least 113 government agencies were impacted by ransomware attacks at an estimated cost of $913 million dollars. These costly cyberattacks are caused primarily by hackers targeting and compromising government vendors and third parties. SecureLink is a third-party remote access security solution for government entities that helps cities, counties, police departments, and government agencies protect themselves from cyberattacks. It also ensures compliance with CJIS security policies, keeps citizen information secure, and increases efficiencies.

Learn more about SecureLink for government!

SECURELINK
THIRD-PARTY SECURITY

Summary

Just remember: PLUMBERS!

Wait, what?

PLUMBERS!

Password-protect accounts and devices

Lock your workstation and screen

Update operating systems

Multifactor-authenticate your accounts and info

Back up your info

Encrypt your personal computer

Report any attacks

Separate work and home lives

SECURELINK THIRD-PARTY SECURITY

govloop

Thank you to SecureLink for their support of this valuable resource for public sector professionals.

Check out our full guide, where we take a deeper dive into these and other cyber topics.