

IT 101 & New Hire Guide

Basics for effectively using technology at CPCS

COMMITTEE FOR PUBLIC COUNSEL SERVICES

Authored by: Daniel Saroff
v.2.05
September, 2021

Table of Contents

INTRODUCTION	3
GETTING HELP	4
VIDEO EDITING	4
BASICS	5
BACKING UP FILES	5
CLOUD STORAGE.....	5
THE WEB AND INTERNET	6
CPCS WEBSITES	6
IT BLOG POSTS, FAQs, GUIDES	6
BLOCKED WEBSITES	6
SPAM FILTERING	7
BARRACUDA	7
OUTLOOK.....	11
EMAIL/CALENDAR	12
FOUR WAYS TO GET YOUR EMAIL AND CALENDAR	12
CPCS EMAIL ON YOUR PHONE.....	12
ANDROID DEVICES.....	12
APPLE DEVICES	14
OUTLOOK EMAIL RESTRICTIONS	16
BOOKING A ROOM THROUGH OUTLOOK	16
OVERSEAS EMAIL ACCESS RESTRICTIONS.....	17
SENDING SECURE EMAIL.....	18
HELPDESK	21
PHONE	23
GENERAL	23
VOICEMAIL TO EMAIL.....	23
CHECK AND DELETE VOICEMAILS FROM OUTSIDE THE OFFICE	25
TIMESHEET OR SSTA.....	26
CONCUR ONLINE EXPENSE PROGRAM.....	26
PRINTERS/COPIERS	27
SECURELY AND CONFIDENTIALLY PRINT TO CPCS XEROX PRINTERS	27
SET A DEFAULT PRINTER	31
SECURITY BASICS.....	34
PASSWORDS	34
CHANGING PASSWORDS ON THE WEB.....	34
MULTI-FACTOR AUTHENTICATION (MFA).....	38
VIRUSES AND MALWARE	41
TIP SHEET.....	42
REMOTELY ACCESSING YOUR PC (GoToMyPC).....	43
USING GoToMyPC	43
WIFI.....	44
CASE MANAGEMENT.....	45
ZELLY.....	45

LEGACY SYSTEMS.....	45
CASEY	45
TRIS.....	45
CMS.....	45
SHARED LAPTOPS– LOGGING IN.....	46
FREE CONFERENCE CALLING	46
LISTSERV ACCESS.....	46

IT 101 & New Hire Guide

Basics for effectively using technology at CPCS

Introduction

The purpose of this guide is to inform you about key CPCS technologies and how to use them.

This guide may be found on the **Information Technology** page of the intranet under the **New Hire** Link (<http://intranet.publiccounsel.net/it/home-2/new-hire/>).

The intranet (<https://intranet.publiccounsel.net/>), especially the IT homepage, is a great resource for assistance.

You will also find most of the HR forms, and Facilities and IT information on the intranet. It's a useful self-service tool for you to find what you need. You can only access the intranet from a device on the network or using GoToMyPC.

As always, if you are unsure of anything technical or need technical assistance, browse to helpdesk.publiccounsel.net for assistance.

Getting Help

When you need help with a problem or question, where do you turn? First, check with your AA – they are a wealth of knowledge and assistance. Then check the intranet (<http://intranet.publiccounsel.net/>) to see if your question has already been answered.

Below are the email addresses for key help resources. Please note, key email addresses are found on your computer wallpaper in the lower right corner.

- helpdesk.publiccounsel.net – **General technology** assistance requests
 - Example: My PC won't boot. I can't access the internet. I can't print
- <https://cpcs.officespacesoftware.com/visual-directory/> – **Facilities** related
 - Example: My chair is broken. The heat is out. Doors don't secure
 - **Office electronic card access**
- hr@publiccounsel.net – **HR**
 - Reasonable accommodation requests (screen readers, voice dictation, etc.)
 - Name changes
 - SSTA (electronic time sheet)
- **Finance** – Questions or issues with the expense program – Concur or Vbill/Ebill
- <http://intranet.publiccounsel.net/IT/> – Find forms, FAQs, training, guidelines, policies, etc.
- zelly@publiccounsel.net – Assistance requests for **Zelly** case management system,
- helpdesk.publiccounsel.net – **Pick**

Video Editing

- Investigators in PDD have received video editing tools, and should be contacted if you need videos edited
 - List is found at <https://intranet.publiccounsel.net/pd/investigator-resources/>
- IT does not have the training or tools to edit videos. If asked, IT will direct the requestor to reach out to a PDD investigator

Basics

Backing up files

CPCS only backs up files stored on the network. So, only store files on your network drive.

If you store files on your PC or laptop, and something happens to your PC or laptop (virus, hard disk dies, etc.), all files on your PC will be lost. IT will not be able to recover them.

All PCs are set by default to store files on the network (L drive, H drive, etc.). If you think yours is not setup correctly, browse to helpdesk.publiccounsel.net for assistance.

Cloud storage

Per instruction of the General Counsel, CPCS **staff may not post client confidential data to the cloud** (e.g., Drop Box, Box, OneDrive, Google Drive, etc.). Due to this injunction, CPCS blocks access to Cloud storage sites.

The Web and Internet

Everyone at CPCS has access to the Web and internet.

Web and internet access are subject to monitoring.

You may find the IT policies on appropriate use on the HR page (<http://intranet.publiccounsel.net/hr/>) in the “Personnel Policies Manual.”

CPCS websites

CPCS has two websites:

- An internal website solely for our staff at <http://intranet.publiccounsel.net/>, and
- An external website for the world at <https://www.publiccounsel.net/>.

The internal web site is only accessible from a device on the network or using GoToMyPC.

IT blog posts, FAQs, guides

IT produces content to help you use technology better. You can find all IT blog posts, FAQs, guides, etc. on the IT page on the intranet at <http://intranet.publiccounsel.net/it/> or under the “Intranet Resources by Section” menu on the intranet.

Blocked websites

We block certain websites. If you need access to a blocked website for client defense, you may request IT unblock the web site. IT needs at least 1 business day notice.

Some site categories CPCS blocks are:

- Porn
- Malware
- Torrent
- Cloud storage (wikis, OneDrive, Dropbox, Box, Google Docs) – per the General Counsel
- Music streaming (Pandora, Spotify, etc. due to bandwidth constraints)
- Gambling
- Gaming

See this post on the intranet regarding temporarily unblocking a website:

<http://intranet.publiccounsel.net/blog/blocked-web-site-and-temporary-access/>.

SPAM Filtering

Barracuda

We filter your incoming email to eliminate SPAM and PHISHING from your mailbox.

HOWEVER, SPAM FILTERING IS NOT A SUBSTITUTE FOR YOUR CARE OR DILIGENCE. BE SKEPTICAL OF ALL EMAILS YOU RECEIVE, ESPECIALLY IF THEY HAVE A LINK OR ATTACHMENT.

Spam filtering is not an exact science, so useful emails may be captured mistakenly. You have the ability to look at emails caught in the filters and release them to your inbox.

Both Outlook (Junk folder) AND Barracuda (our primary tool) capture emails into SPAM. So, you need to check in both locations if you wish to look at your SPAM.

Twice a day, staff receive email listing email captured in **Barracuda** SPAM servers. You may:

- **Deliver** – this will send the trapped email to your mailbox.
- **Whitelist** –allow this email address in the future and deliver.

You may check the Barracuda SPAM servers from anywhere - work, home, mobile device - using your CPCS Windows login name and password.

Recommended: This four-minute YouTube video explains Barracuda simply and easily: <https://www.youtube.com/watch?v=zw1g9pnRu-M>

Managing Barracuda

1.Login

The login at <https://ess.barracudanetworks.com>

1. Username: CPCS email address
2. Password: CPCS PC password
 - **Note:** When you change your PC login password, you will need to use the new password to access Barracuda
3. Once you login, you have access to the “Message Log” where you manage quarantined messages and set preferences (like frequency of notification) or whitelist someone

2. Spam notifications

Around 3am and 2pm daily, **if you have new SPAM**, you will receive an email (you may change this frequency) listing messages in caught in the SPAM filters (**Figure 1**).

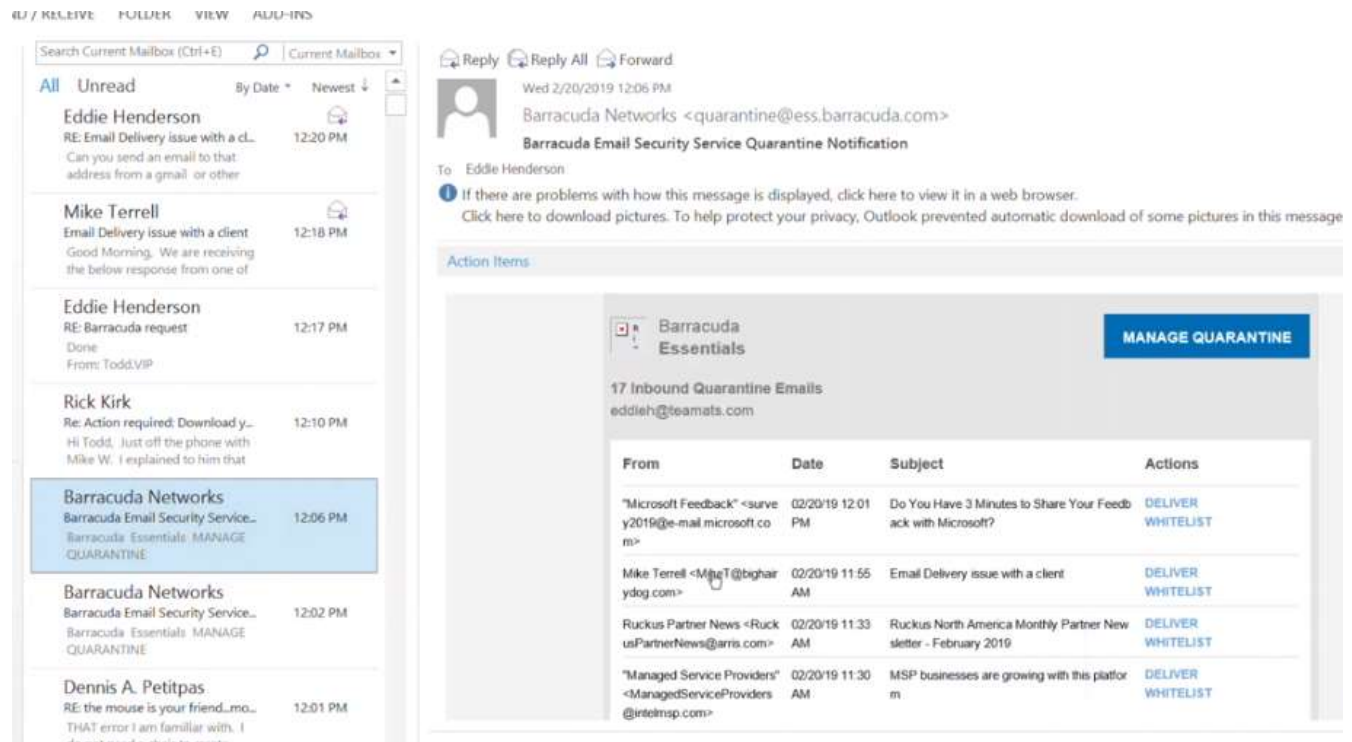
From this email you may choose to “Deliver” a message or “Whitelist” the sender.

- **Delivering:** Puts the email in your mailbox

- **Whitelisting:** Delivers the email AND instructs the system not to quarantine in the future

Note: Quarantined messages are deleted automatically after 30 days.

Figure 1: Quarantined Email Notification



3.Change notification frequency

- Go to your Message Log
- Go to **Settings > Quarantine Notifications** page
- Select **Scheduled** and click and drag to set the day and time for notification email delivery (**Figure 2**)
- Click a selection to clear a selection
- Click **Save Changes** to save your settings
- Select **Never** if you do not want to receive quarantine notifications

Figure 2. Set Quarantine Notification Interval.

Notifications will be sent at any time within the hour block chosen.
Click and drag to select. Hold Ctrl while dragging to unselect.

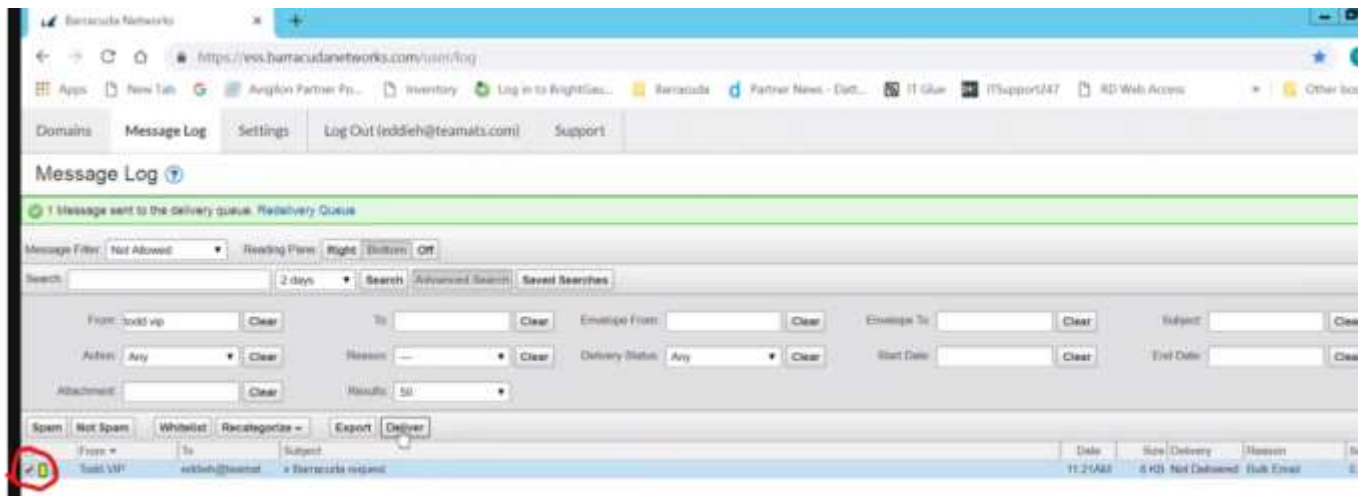
You may check your spam quarantine any time you wish (e.g., someone tells you they sent a critical email 15 minutes ago, and it isn't in your inbox) by logging in to your account.

- Login to your account to use the Message Log to manage email
- The Message Log page displays all email messages quarantined as potential spam
- You can filter messages by using the drop-down menu (**Figure 3**)
- **All** – show all messages even ones that have been delivered to your inbox
- **Allowed** – show only messages that you allowed to go to your inbox
- **UI Delivered** – an administrator manually delivered the message to your inbox
- **Not Allowed** – show messages that are held and not delivered
- **Blocked** – known spam sites or domains or flagged as hosting a virus
 - May only be released by the helpdesk. IT will unblock only if demonstrated safe
- **Deferred** – the message is ready to send, but an issue (e.g., email servers down) blocked it from being delivered
- **Quarantined** – held until you release them

Managing your messages:

- Select message(s) by clicking the box to its right (red circle), and then select the action you wish to take. **(Figure 4)**. To select all messages, select the check box at the top of the Message List. Actions are:
 - **Spam** – Selected messages are sent to Barracuda Central for analysis. Must select “Not spam” for them to be delivered
 - **Not Spam** – mark messages as not Spam and send
 - **Whitelist** – Senders are whitelisted. They will no longer be caught in the filter
 - **Note:** You cannot whitelist **blocked** messages
 - **Deliver** – The service attempts to deliver the selected messages to your mailbox. If a message is successfully delivered, the Delivery Status changes to **Delivered**

Figure 4. Managing messages



5. Whitelisting an email address or domain (or block an annoyance).

Sometimes you will have a person whose emails you don't ever want caught in the Barracuda Spam filters. For such a person, you can whitelist their email address.

WARNING: If you whitelist someone's email address and they send an infected file or they were hacked, the Spam filters won't stop it and you risk infecting the agency. So, do this only rarely.

To whitelist (See Figure 5):

- Go to **Settings** and click **Sender Policy**
- Type the email address and from the **Policy** drop down select **Exempt**
- Under **Actions** click **Add**
- To blacklist a person (permanently block them)
- Follow the same steps as above but select **Block** or **Quarantine** from the **Policy** drop-down

Figure 5. Whitelisting (or black listing) email addresses

Message Log **Settings** Log Out (dsaroff@publiccounsel.net) Support

Quarantine Notification **Sender Policy** Linked Accounts

Sender Policy ?

Specify whether to Block or Exempt messages coming from a specific email address or domain.

Sender	Policy	Comment	Modified	Actions
dsaroff@publiccounsel.net	Exempt			Add
dsaroff@pobox.com	✓ Exempt		10:09 am	Remove
vancord.com	✓ Exempt	Vancord	9:37 am	Remove

Outlook

If email you want keeps going to your Outlook “Junk Email” folder, whitelist those emails so it will stop.

The steps are:

1. Go to the Junk Mail Folder
2. Find the email you wish to whitelist
3. Right-mouse-click on the email and select Never Block Sender

Junk Email

FROM	SUBJECT	RECEIVED
TradePub.com	Daniel, I	Software

Tue 11/19/2019 08:53

- Copy
- Quick Print
- Reply
- Reply All
- Forward
- Mark as Unread
- Categorize
- Follow Up
- Find Related
- Quick Steps
- Rules
- Move
- OneNote
- Ignore
- Junk
- Delete
- Archive...
- Save to Evernote
- Convert to Adobe PDF
- Append to Adobe PDF

- Block Sender
- Never Block Sender
- Never Block Sender's Domain (@example.com)
- Never Block this Group or Mailing List
- Not Junk
- Junk E-mail Options...

Email/Calendar

We use Microsoft Outlook as our PC mail and calendar client and Microsoft Exchange on the server. You can get your calendar and email on other devices than your work PC.

Four ways to get your email and calendar

1. **On your work PC** – For [instructions](#) on how to use Outlook calendaring and email, see guides on the intranet IT page (<https://intranet.publiccounsel.net/>)
2. **Webmail** – Work email and calendar accessed from any web browser on any device (personal laptop or PC, smart phone, tablet). Login is your **work email address** and **PC password**. The web address is:
 - <https://office.office365.com>
3. **GoToMyPC** – You may login to your computer remotely through GoToMyPC. Instructions on GoToMyPC are later in this document and on the intranet
4. **iPhone, Android phone or tablet**
 - CPCS emails and meeting invitations can be accessed on your mobile device. **You must use the Outlook App on your device** (instructions below)
 - MaaS360 was discontinued in May 2021

CPCS email on your phone

Android Devices

1

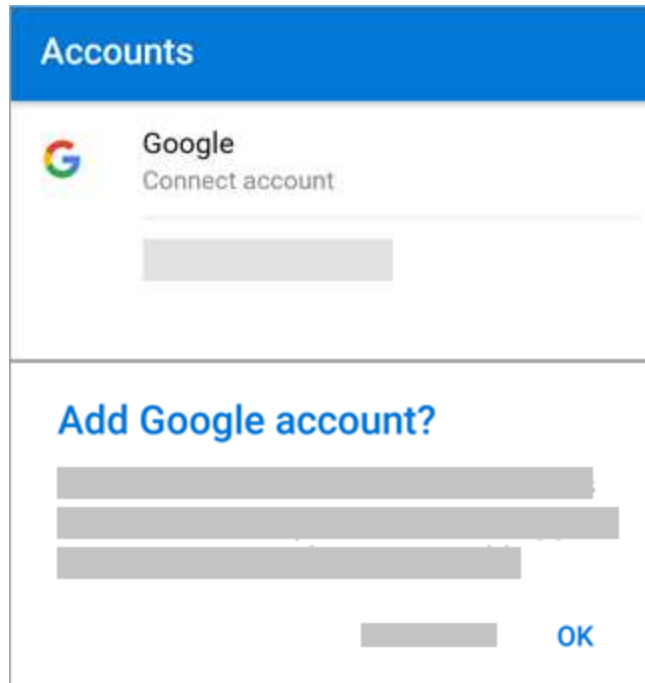
Install the **Outlook for Android** app from the [Google Play Store](#) and then open it.

Tap **Get Started** if this is your first time.

Otherwise, to add another email account, open the **Menu**  > **Settings**  > **Add Account** > **Add Email Account**. Then skip to step 4 under [Set up another email account](#) below.

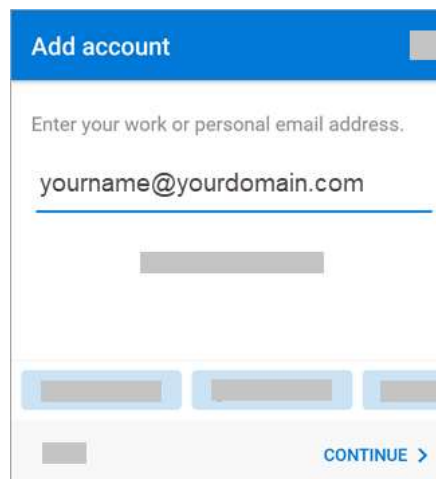
2

Outlook may detect your Google accounts. Tap **Skip**



3

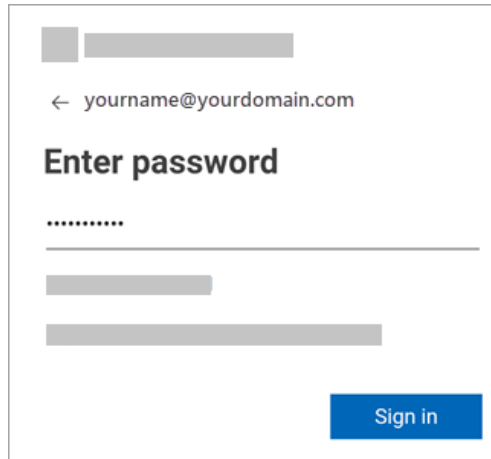
Enter your full CPCS email address, then tap **Continue**.



4

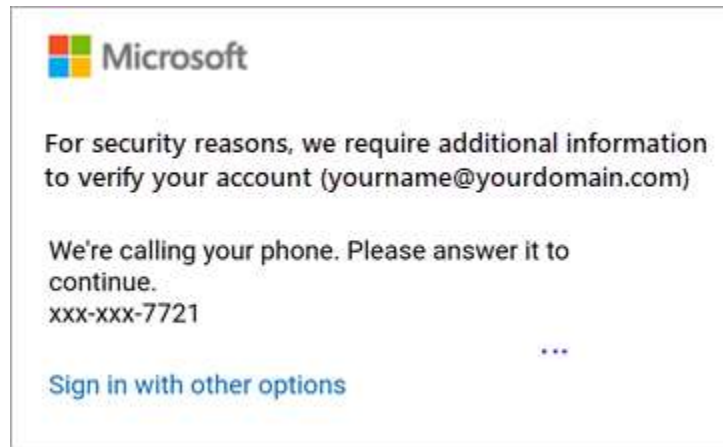
Enter your email account password and tap **Sign In** or **Next**.

Note: This is the password you would use to access your desktop when at the office



5

If multi-factor authentication is enabled, verify your identity.



You have successfully configured Outlook to receive CPCS email.

You must wait up to 30 minutes for email to begin flowing to your device.

If mail does not begin to flow after a half hour or if you have any further questions or concerns, browse to helpdesk.publiccounsel.net.

Apple Devices

1

[Download Outlook for iOS from the iOS App Store](#) and then open it. The icon looks like this:



2

If it's your first-time using Outlook for iOS, enter your full CPCS email address, then tap **Add Account**.

If not, open the **Menu** > tap **Settings**  > **Add Account** > **Add Email Account**.

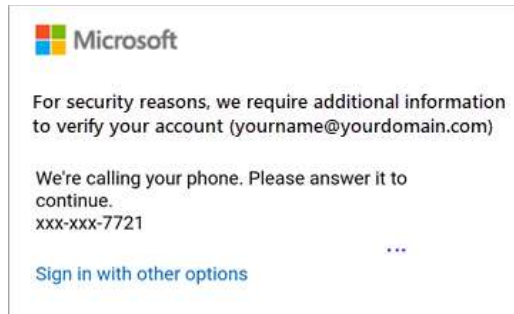
3

Enter your CPCS email account password and tap **Sign In**.

Note: This is the password you would use to access your desktop when at the office

4

If multi-factor authentication is enabled, verify your identity.



5

Accept any prompts for permission you may receive.

Swipe through the features and you're now ready to get CPCS email on Outlook for iOS!

You must wait up to 30 minutes for email to begin flowing to your device.

If mail does not begin to flow after a half hour or if you have any further questions or concerns, browse to helpdesk.publiccounsel.net.

Outlook email restrictions

- **Social security numbers:** Transmittal of social security numbers are blocked. If you wish to send a document with a social security number to an outside party, you need to send it via **Secure Mail** (see section, below)
- **Attachment File Size.** Maximum sized attachment that can be sent or received is 20MB
- **CPCS email for personal use:** This is against agency policy. Do not use a CPCS email account for personal purposes. We retain ALL CPCS emails and they are considered public records

Booking a room through Outlook

To reserve a room, you must book it through your Outlook calendar. Instructions can be found in an IT blog at <http://intranet.publiccounsel.net/blog/how-to-book-a-room/>.

Overseas email access restrictions

CPCS blocks **access** to CPCS email from outside the United States.

What this means:

- If you travel outside the United States, you will be blocked from **accessing** CPCS mail (on the Web or phone or laptop)
 - For example, if you are in Peru, you will be **unable to access** your email (to send or read emails) until you return to the United States
- Your mailbox still receives or sends email anywhere in the world
 - If a client emails you from Peru, you will receive it, and you can respond to it

Why we are doing this:

Daily there are access attempts on our email servers (and other services) from around the world.

Since our representation is in the US, it should be rare that any member of staff needs to access email from outside the US.

By restricting access, we help further protect our environments from hackers.

Exemption:

We understand there are rare circumstances where staff are **overseas on CPCS business** and need access to their email.

If you need a temporary exemption for this purpose, you must request it from your Managing Director (or equivalent) and have them reach out to the CIO.

The request needs to be submitted 5 business days in advance of the trip. The request needs to have a start and end date.

Sending Secure Email

As a Commonwealth agency and a law firm, we are required to protect personally identifiable information (PII), such as social security numbers, date of birth, and confidential information. Email can be hacked or mis-directed, so protecting email containing PII or confidential information is critical.

To protect sensitive email or attachments, CPCS implemented a system to send secure email using Barracuda. Following are instructions on its use.

You only need to use it when transmitting PII or particularly sensitive information **outside CPCS**. It can be used with clients, DAs, experts, etc.

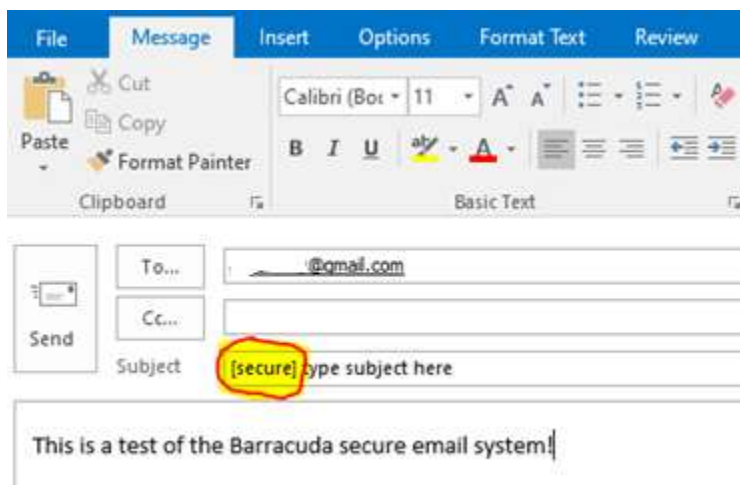
NOTE:

- Notify the recipient IN ADVANCE that they will receive a secure email so they don't delete it as phishing or spam
- Notify them that it will require login to a secure web site to view the email and attachment
 - This means they will need to create a free account
- The secure email simply contains a link to the secure web site where the email and attachment may be read

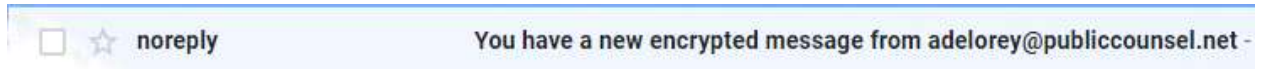
Instructions:

To send a secure email:

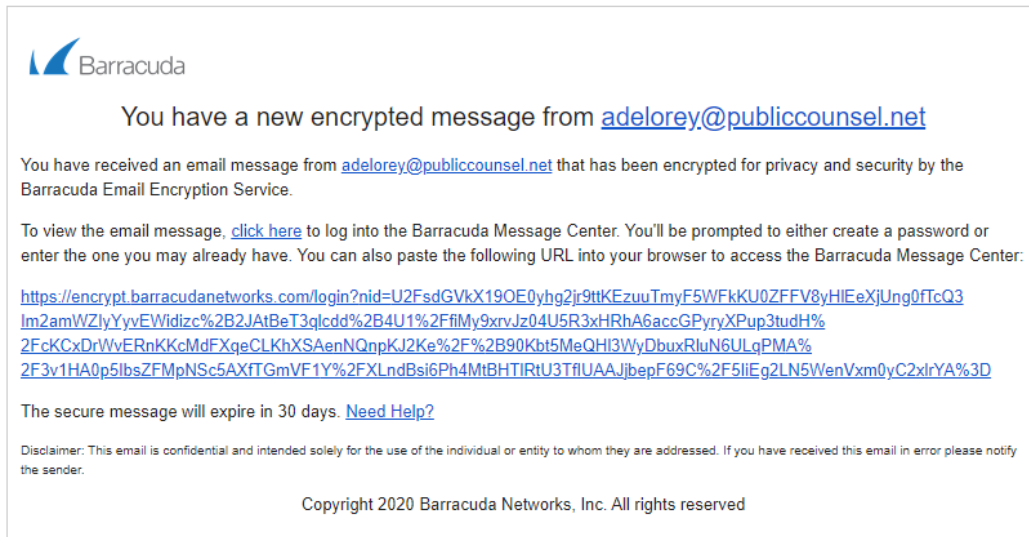
1. To send a secure mail type **[secure]** in the subject line **before** you type your subject text. See example, below



2. Type your email body text and add any attachment as with any normal email
3. Click send. The system will notice [secure], hold your email, and send an email with a secure session link to the recipient
4. The recipient receives an email that appears similar to this:



5. The body of the secure email (below) directs the recipient to click the link to review the email



Receiving party

1. On **first-time** receipt of a secure email, the recipient must create an account
2. They create an account with Barracuda by clicking the link in the email
3. The account creation is a simple one-step process of choosing a password
 - o Remind them they need to remember their password

Account Settings for [redacted]@gmail.com

4. Once logged in, they are brought to their secure messages inbox



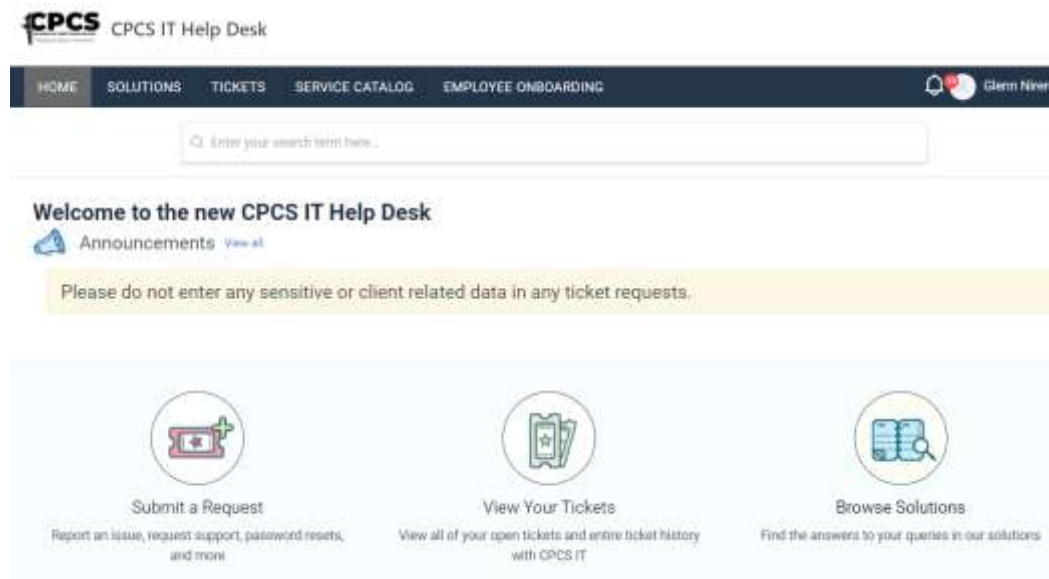
5. Click the message to read and view and download attachments



6. If the recipient uses the Barracuda reply function, it will reply through the secure app. So, if they use the reply option in Barracuda, you will receive a notification to login to the secure app to read it. If you don't want them to reply in the Barracuda app, you will need to notify them

Helpdesk

The CPCS IT Helpdesk ticketing system can be accessed from any browser by going to <https://helpdesk.publiccounsel.net/support/home>



You have three options: submit a request, view your tickets, and browse solutions.

Before submitting a ticket, please browse the solutions to see if there is information to save you from submitting a ticket. There are useful tips for issues with things like remote desktop, email and more.

If you do not see a solution there, please submit a ticket by:

1. Clicking on the submit a ticket icon



2. Then select category

SERVICE CATEGORIES

- IT Infrastructure and Sup...
- Programming

IT Infrastructure and Support

Email, File/Folder Access, GoToMyPC, Hardware, Network, Phones, Printers, Software Install, password resets, login issues, Virus/Phishing

Programming

New Feature Requests, PICK, Reports, Request a new program, WordPress

- Pick a category that best describes your issue



- Best contact phone number is a required field.** Fields with a red * are required. You may select "Request for someone else" by adding their email address

Email
Any issues sending or receiving emails including Outlook on your desktop, Outlook online, Exchange

Best contact phone number *

123456789

Alternate phone number

Date *

12-09-2021

Describe your issue *

I have an issue with Outlook

Please select an issue category *

Outlook

Location *

Boston - 75 Federal Street 5th floor

Department *

GAFL - 3600

Items Requested

Email

Requester *

greenberg@publicaccount.net

☒ Request for someone else

Request for *

Attach a file

Once you submit that form someone from IT will reach out to you.

Phone

General

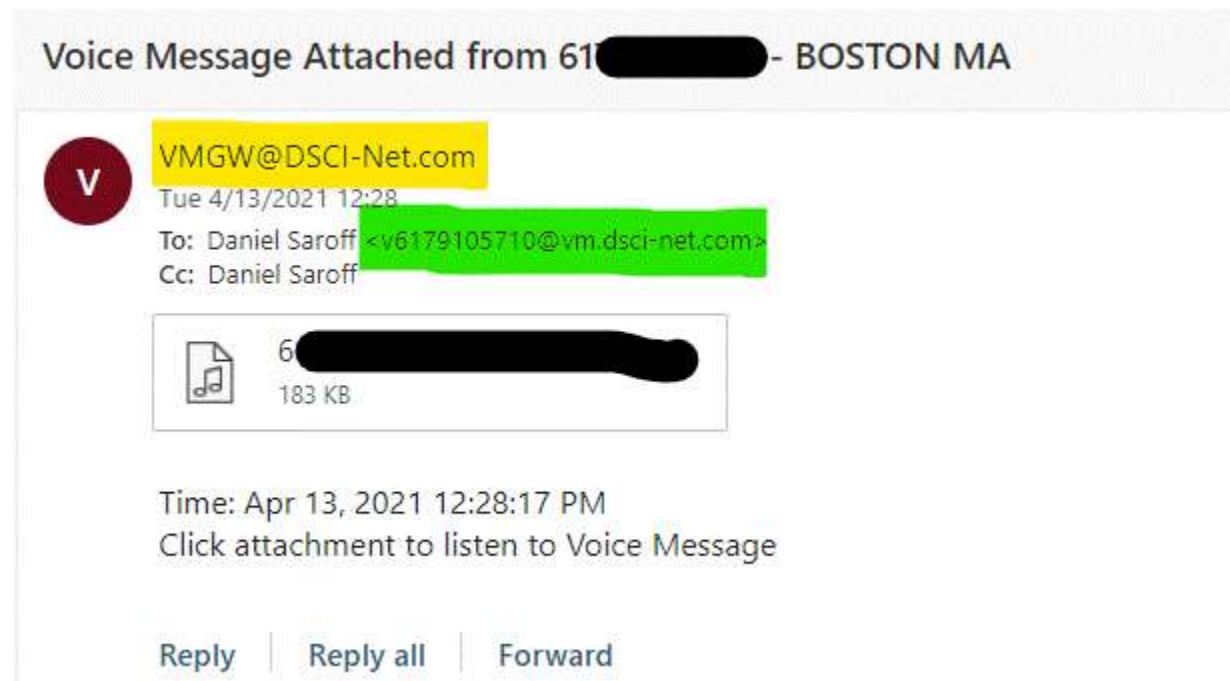
Your desk phone runs across the network, just like your PC. It is a voice over internet protocol (VoIP) device. A key advantage of this is voicemails are sent to your PC as email attachments. So, you can listen to them from your email by double clicking them to open the file.

- If this isn't occurring, please contact the Help Desk.

Voicemail to Email

To recognize voicemails to email from CPCS, note these key elements:

- Black: lists the phone # that sent it in the subject & in the attached mp4
- Yellow: comes from the email address of our VoIP provider
- Green: the "To:" field should have your name followed by an email address that contains your work phone number.



Just like a PC, sometimes your phone may hang. If your phone hangs, this means your PC will lose network access (because your PC is hooked through your phone). If this happens, unplug the Ethernet cable from your phone. This is the cable that runs from your telephone into the wall.

- If your PC can't access the internet check whether your phone is working. If not, reboot your phone.

You can find links to the quick reference guide and the detailed user guide for your phone on the IT Resources page (<http://intranet.publiccounsel.net/it/it-resources/>) under the "IP Phone" heading partly down the page or

- Cheat Sheet:
<http://intranet.publiccounsel.net/it/wp-content/uploads/sites/2/2014/10/IP-Phone-400-410-user-guide.pdf>
- Full Manual:
http://intranet.publiccounsel.net/it/wp-content/uploads/sites/2/2014/10/polycom_vvx400_410_userguide.pdf

Check and delete voicemails from outside the office

If you don't delete voicemails from your work voicemail box, it will eventually stop accepting new messages as it fills-up.

When you delete a voicemail **email** from your email, it does not delete it from your phone inbox. Unless you login in to your **phone** inbox to delete voicemails, your voicemail box will fill up and be unable to accept new voicemails.

Below are instructions on how to login to your voicemail from outside the office and check and delete old voicemails.

1. Look up **YOUR Group Portal Number** (table, below)
2. Call the **YOUR Group Portal Number**
3. At the greeting, dial your extension and press the # key
4. Enter your passcode and press #
5. Listen to and delete unneeded voicemails.

Offices	If your phone number starts with:	Your office's Group Portal Number is:
Boston/Bromfield	617-910-	617-910-5899
Formally Boston/Congress Street	617-209-	617-209-5599
Brockton 144 Main	508-484-	508-484-5489
Brockton 221 Main	508-484-	508-484-5899
Fall River	508-484-	508-484-5799
Framingham	508-283-	508-283-5423
Formerly Hadley	413-355-	413-355-5307
Hyannis	508-815-	508-815-5065
Lawrence	978-855-	978-856-6999
Lowell	978-856-	978-856-6199
Malden	781-652-	781-652-4399
New Bedford	508-617-	508-617-5649
Northampton	413-588-	413-588-5079
Norwood	781-381-	781-381-5240
Pittsfield	413-449-	413-449-5539
Quincy	508-484-	508-484-5925
Roxbury/Malcolm X	617-318-	617-318-5529
Roxbury/Palmer ST	617-516-	617-516-5849
Salem	978-219-	978-219-5499
Somerville	617-607-	617-607-5799
Springfield	413-355-	413-355-5343
Worcester	508-443-	508-443-5499

Timesheet or SSTA

You submit your timesheet weekly. **IT does not provide support for the timesheet system** (also called Self-serve Time and Attendance or SSTA). Please contact your HR representative or SSTA support.

On the intranet (<http://intranet.publiccounsel.net/hr/self-service-time-attendance/>), HR has created a page with training and information links on using SSTA.

You reach SSTA through <https://www.mass.gov/employee-self-service>.

Concur Online Expense Program

Concur is a cloud-based expense program used by CPCS and sponsored by Finance. **IT does not provide support for Concur.** If you have difficulties with Concur, please contact Finance.

You reach Concur through <https://www.concursolutions.com>

Printers/copiers

You should be able to print to the printers in your office. If you can't, please contact the helpdesk for support.

If the printer/copier machine is not working, please have your AA contact Xerox.

If the printer/copier machine is out of supplies, please contact your AA to order supplies (print cartridges, toner, paper, etc.).

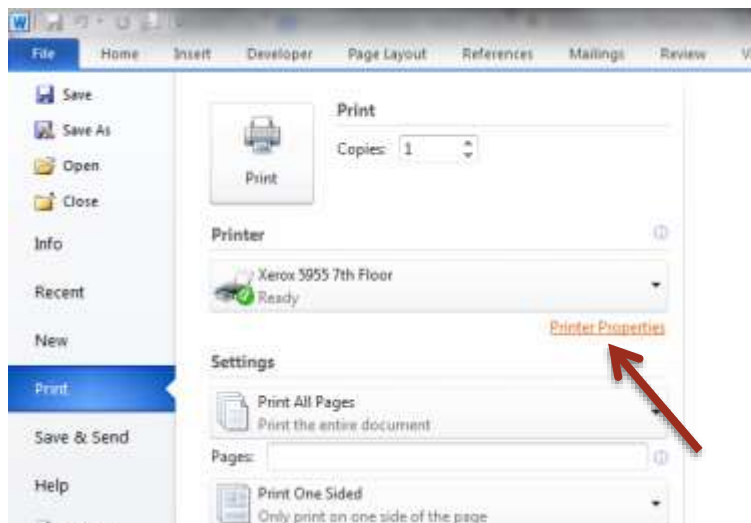
Securely and Confidentially Print to CPCS Xerox Printers

Xerox printers support **Secure Print**, which holds document printing until you enter a password at the printer.

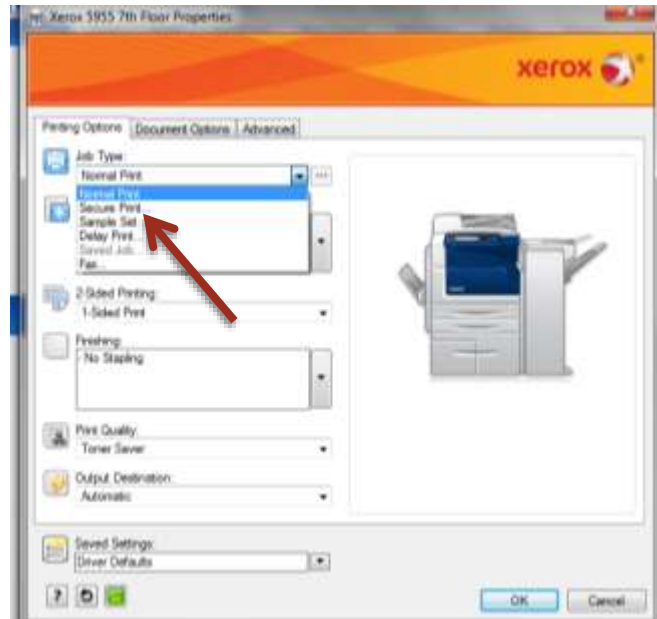
This is useful if you need to print confidential or sensitive documents to an office printer, because it only prints the document when you are standing at the printer to receive it.

To use Secure Print:

1. Open the print dialog in a program such as Adobe Acrobat or Microsoft Office
2. Select the Xerox printer and click on the **Printer Properties** button or link



3. Change the **Job Type** drop-down box from Normal Print to **Secure Print**



4. Enter a password from 4-10 digits

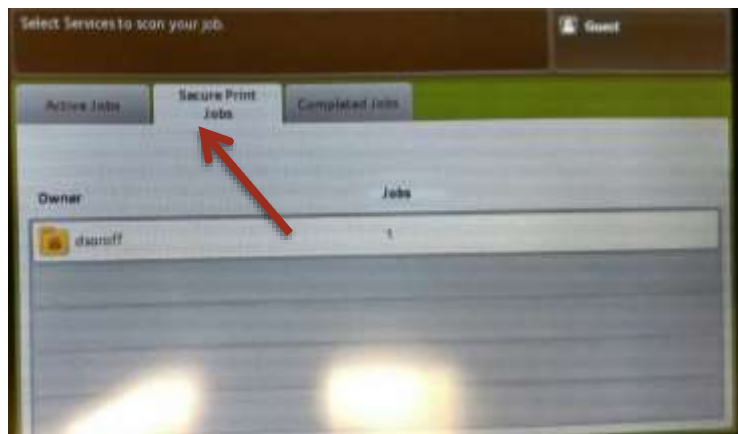


5. Click **OK** and **OK** and then **Print**

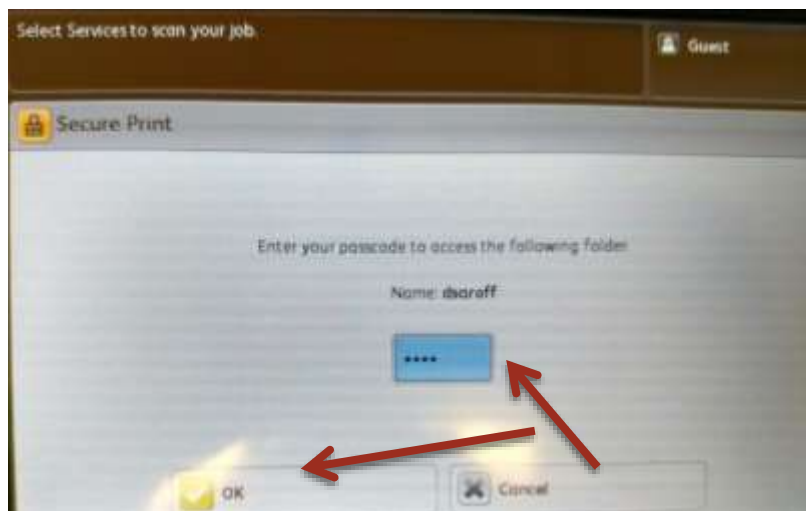
6. Go to the printer and press the **Job Status** button on the control panel



7. Tap the **Secure Print Jobs** tab and look for your name

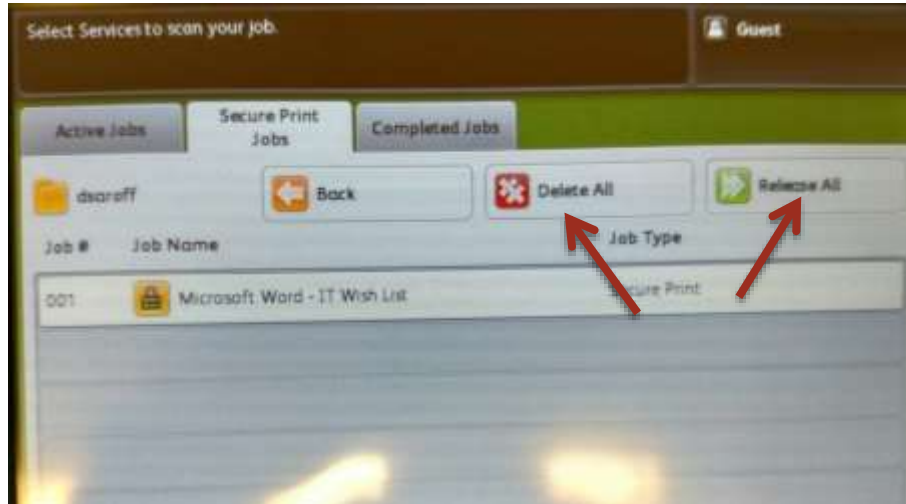


8. Enter your password (any password you like) and hit **OK**

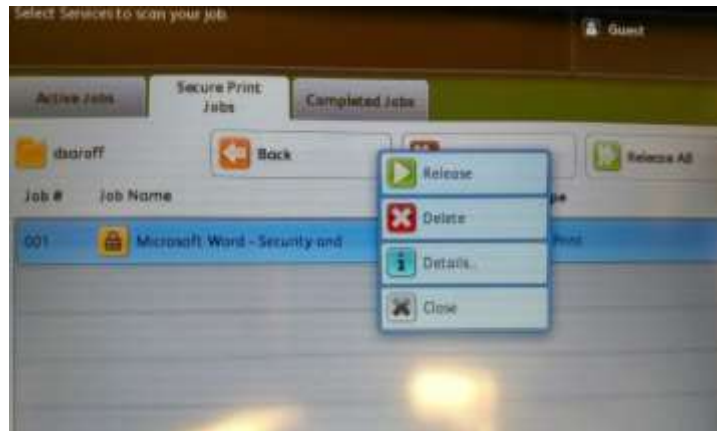


9. You will be taken to your queue, where you will have the choice to either print all (**release all**) or **delete all** or print one or delete one (if you have more than one document tap it to show popup menu with choices).

Print or delete all:



Print or delete one:



10. When you are done, press the **Services Home** button on the control panel to exit

11. REMEMBER:

When you close the application (e.g., Word), printing automatically reverts to “normal”, not “secure.” If you keep the application open, all printing will be “secure” unless reset it to normal (see #2 and #3, above)

12. If you forget a document in the printer, after 72 hours it will be deleted.

Set a default printer

NOTE: Each printer is labelled with its name (location and model number).

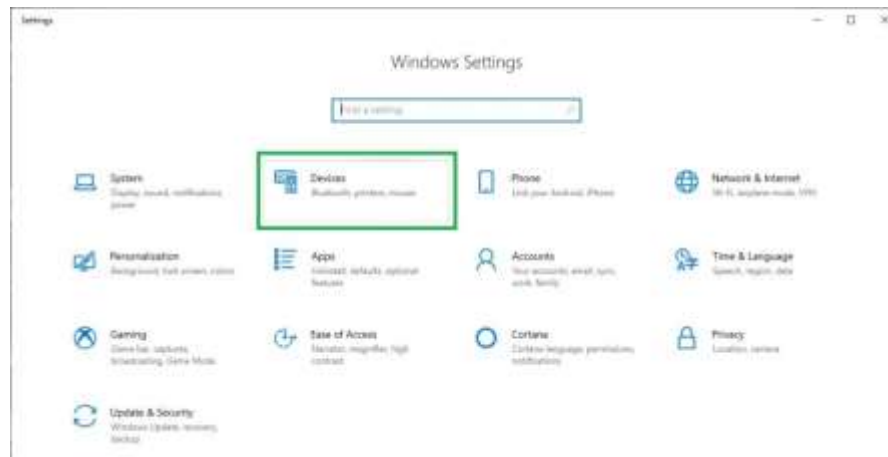


To select a default printer, follow these steps.

1. Navigate to printer settings.
 - Click on the **Start button**, then **Settings (gear icon)** to reach the Windows Settings screen.
 - You can also go to screen using the keyboard shortcut **Windows key - I**.



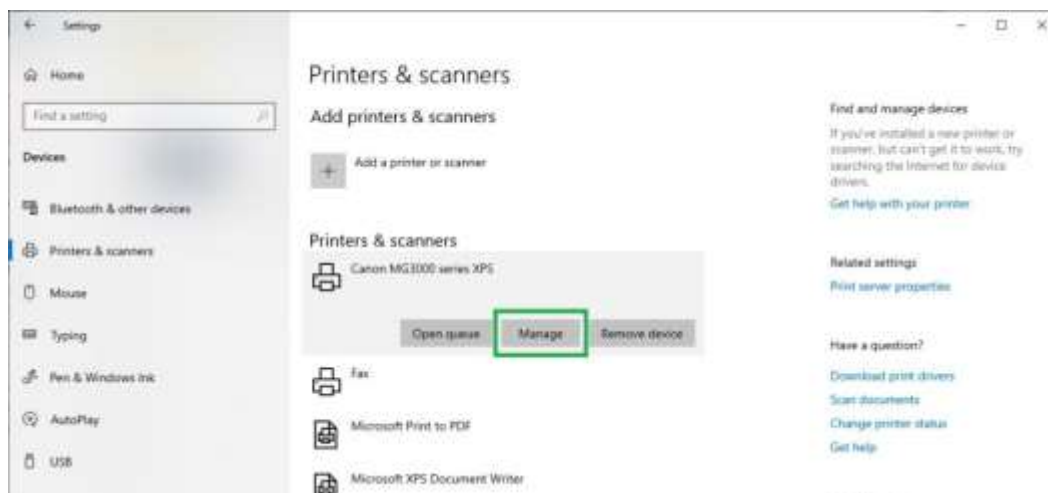
2. Click Devices.



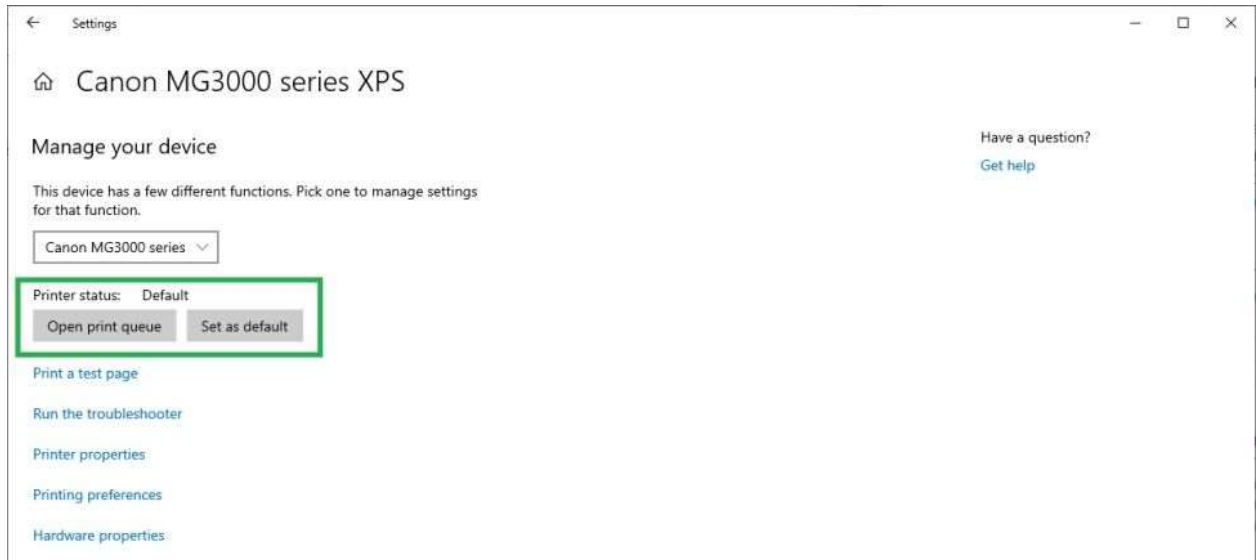
3. Click Printers and scanners on the left side



4. Select the printer you want and click Manage.



5. Click **"set as default."** You can confirm the change was successful by looking at the printer status. If there is no "set as default" button, that means your printer is already the default.



Now any program you print will default to the printer you designated.

Security basics

Passwords

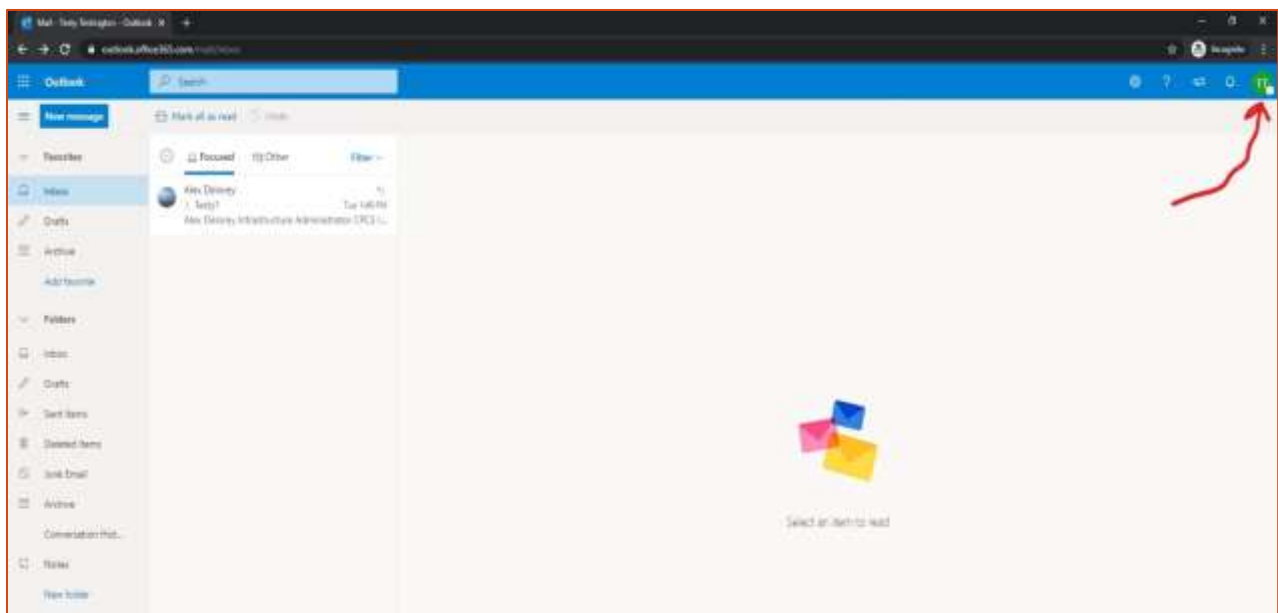
Your Windows password changes every six months. You will be notified two weeks in advance. You can change your password from your PC or via GoToMyPC or from Outlook Web. When it changes, you will have to update it on any phone or tablet you use to access CPCS email or WiFi. You will also need to change it in the Outlook phone app.

The password format for your Windows login is:

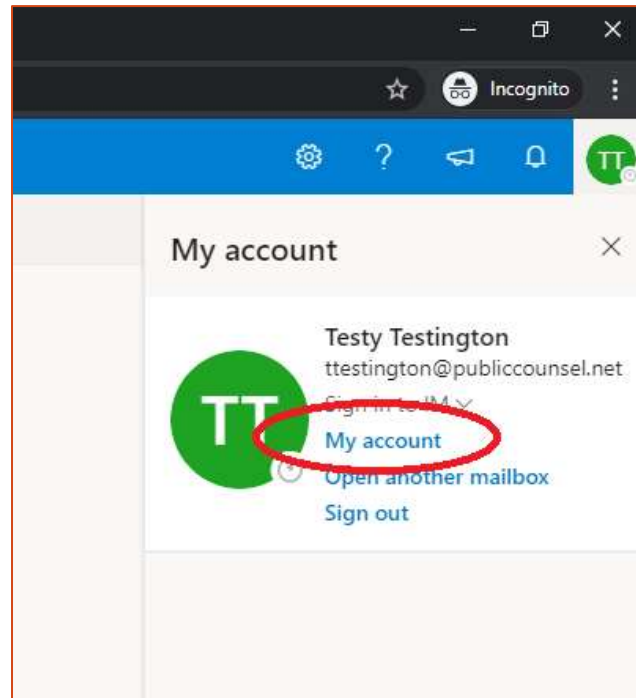
- Minimum of 10 characters and contains characters from three of the following types
 - English uppercase characters (A through Z)
 - English lowercase characters (a through z)
 - Numbers (0 through 9)
 - Non-alphabetic characters (for example, !, \$, #, %)
- Passwords cannot contain your account name or parts of your name
- Don't share your passwords with anyone.
- Password must be unique (you may not use it for any other site).

Changing Passwords on the Web

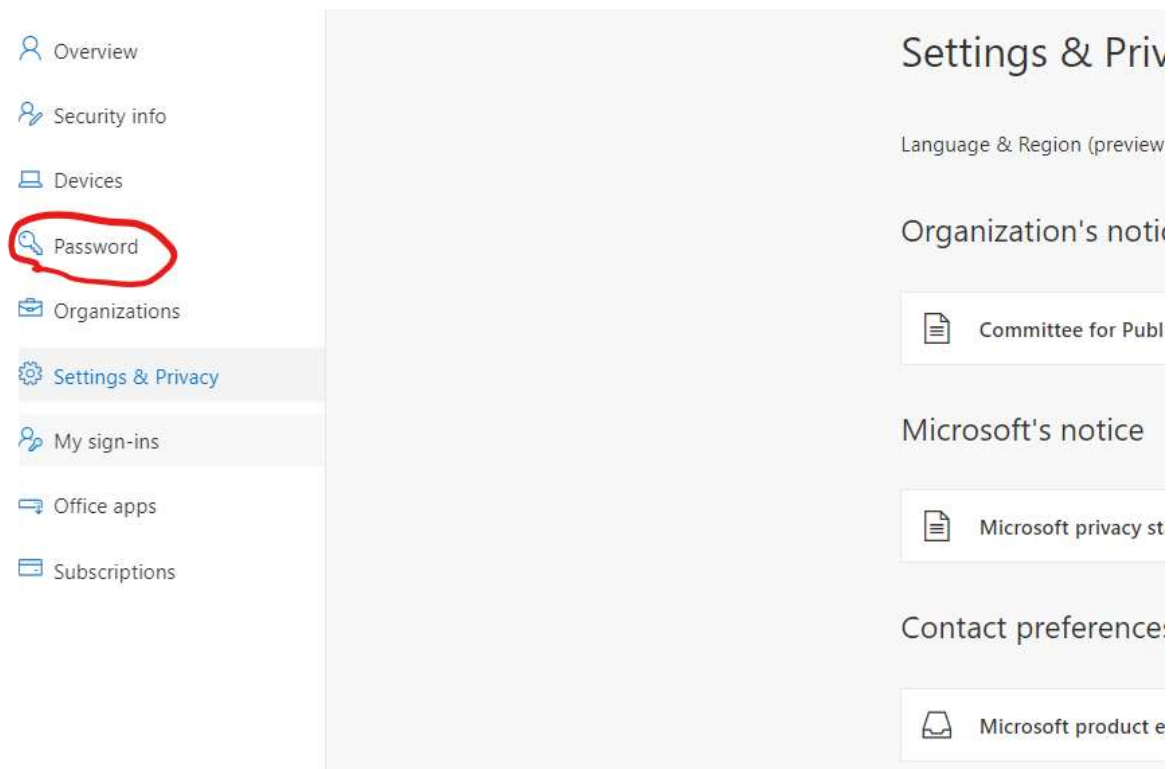
1. Go to website **mail.office365.com**. Login using your CPCS email address and password
2. In the upper right-hand corner, click on your account circle.



3. This circle will have either your initials or your Outlook profile photo
4. Click **My account**



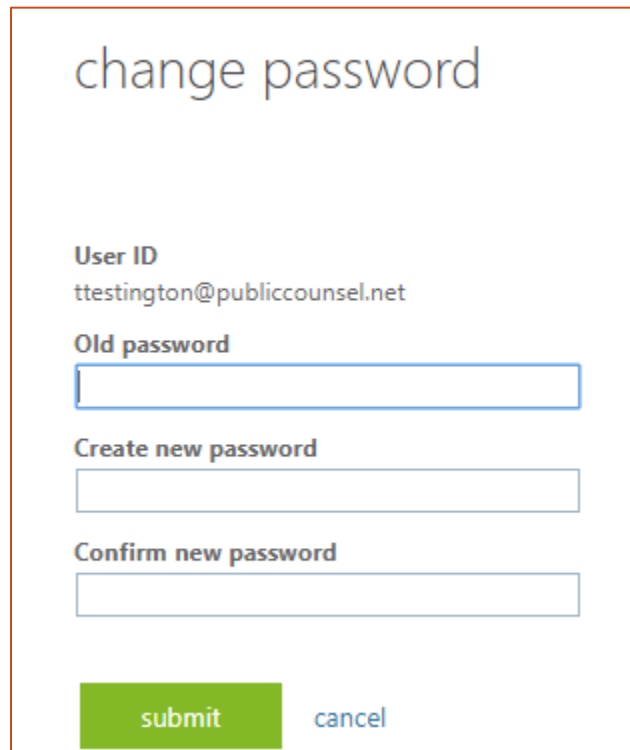
5. After clicking on **My account**, click on **Password**



6. On the **Password** page, enter your old password, and your new password and confirmation, and click **submit**

Password requirements:

- You cannot reuse any of your past 4 passwords
- **Password Length:** Minimum of 10 Character
- Must contain at least **3 of the following 4** types:
 - English uppercase characters (A through Z)
 - English lowercase characters (a through z)
 - Digits (0 through 9)
 - Non-alphabetic characters (for example, !, \$, #, %)



change password

User ID
ttestington@publiccounsel.net

Old password

Create new password

Confirm new password

submit cancel

7. You have changed your password. **Most likely you will be prompted to sign in again with your new password**
8. You must reboot your work PC

- a. Click the Start button menu on your computer.  or 
- b. Click the **Power** icon and select **Restart**. This will reboot your PC. You can do this in the office or over GoToMyPC
- i. When you restart your PC over GoToMyPC, you will be logged out of GoToMyPC. Wait five minutes for the computer to reboot, and then try logging back into GoToMyPC

NOTE: If you have not used webmail before, you will need to answer two questions (preferred time zone and language). **Once answered, you will be brought to an Outlook online tutorial. The tutorial may be skipped by hitting the X.**

Multi-factor Authentication (MFA)

What is MFA?

Multi-factor authentication (MFA) is a security measure. You've probably experienced this when accessing your banking website, Google email, or other secure websites.

When you try to login to your CPCS accounts (Outlook, Zelly, OfficeSpace, etc.) from a different device, it will send a text to your cell phone (or an app) to verify it is you logging in. Just like your bank. This will also happen if the login times-out due to disuse (one-hour) or randomly.

Note: See the IT intranet page for instructions on how to *CHANGE* your MFA method once setup.

Purpose:

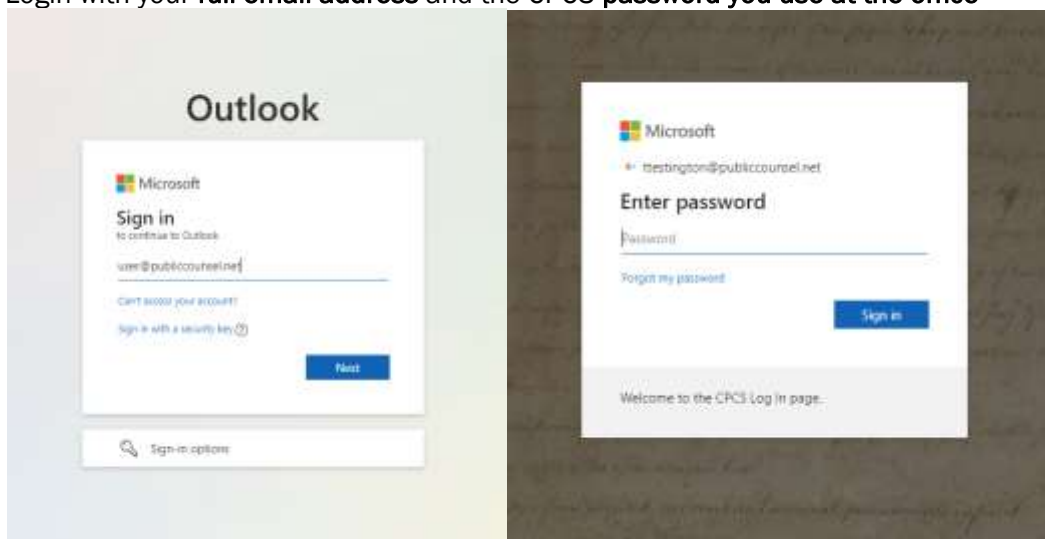
To confirm that it is you trying to access your account (and not a hacker who stole your username and password).

Setup MFA:

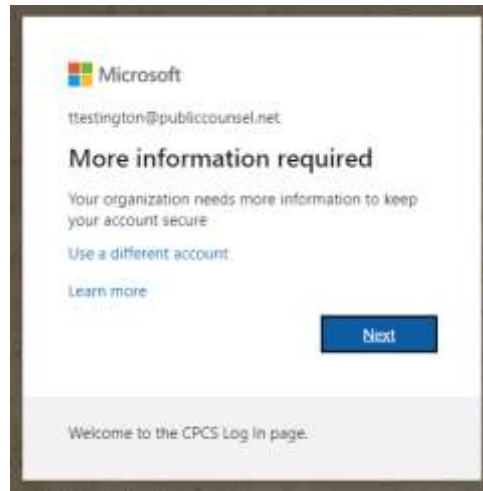
When MFA is activated on your CPCS Microsoft account, you need to immediately set it up to log into your email and other CPCS online services (Zelly, OfficeSpace, etc.).

Steps:

1. Go to **mail.office365.com** in any web browser (**DO NOT** use Internet Explorer)
2. Login with your **full email address** and the CPCS **password you use at the office**



3. Click **Next**



4. **Choose your authentication method, i.e., how the app provides you with a verification code.** The (below) screenshot shows the method **where the verification is sent as a text message** to your cell phone. There are three options to choose from. #1 or #3 are recommended.

Your three options:

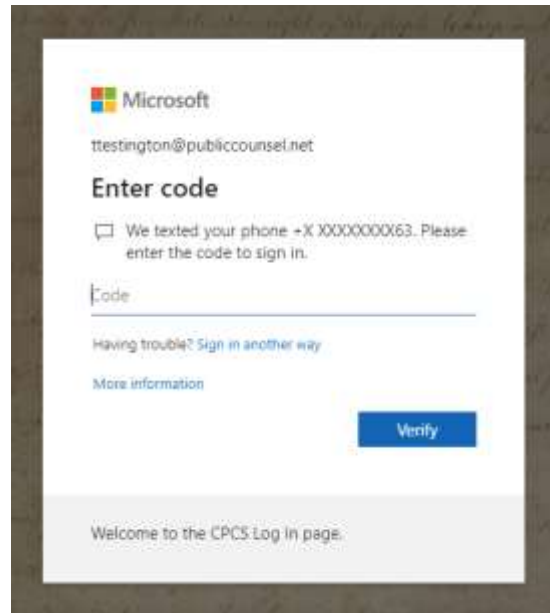
1. **Authentication Phone** (Receive code on your cell phone)
 - a. Receive a text message or
 - b. Receive a phone call. You will need to answer
2. **Office Phone** - Receive a call on your office phone. You will need to answer
3. **Mobile App** - Receive a code though the Microsoft Authenticator App installed on your phone (you must install it from your phone's app store)

Choose your preferred contact method, click **Next**, and confirm your setup. You are now setup with MFA.

A screenshot of a Microsoft account setup page titled 'Additional security verification'. It says 'Secure your account by adding phone verification to your password. View video to know how to secure your account'. The main heading is 'Step 1: How should we contact you?'. There are two dropdown menus: 'Authentication phone' and 'United States (+1)'. A text input field contains 'YOUR CELL PHONE # HERE'. Below these is a 'Method' section with two radio buttons: 'Send me a code by text message' (selected) and 'Call me'. A blue 'Next' button is on the right. At the bottom, it says 'Your phone numbers will only be used for account security. Standard telephone and SMS charges will apply.' and '© 2021 Microsoft Legal | Privacy'.

Using MFA:

When accessing your CPCS Microsoft Account **from a different device** or **after logging-out of a CPCS account** (like logging out of Zelly or Outlook) or **randomly**, after you enter your username and password, you will see a screen, below, prompting you to enter your MFA code.



WARNING: Do not enter the code unless you are actively trying to access your account and were notified you would need an access code to start. If you receive a code when you are **not** trying to access your account, do **not** enter the code; immediately contact the helpdesk.

Viruses and malware

We scan all files with antivirus software, but just like a vaccine, it doesn't catch everything. Too many viruses are being created too quickly for antivirus companies to keep up.

You are a key line of defense in protecting CPCS. Follow the tips, below, and you will help CPCS defend itself against Cyber-attacks (and they will help you at home, too!).

- When reading and email, go in with the mind-set that, 'I will not click a link or attachment'
- When in doubt about an email or web site, ask IT (helpdesk.publiccounsel.net)
- Don't assume antivirus software catches everything
- Don't click links or attachments from people you don't know. **Period**
- Don't click links or attachments if you are not expecting an email with one
- Check the email address makes sense for the sender (hover your cursor over the To: name in the email and it will show you their email address. If it doesn't match the user, it's a hoax)
- Don't click generic emails ("You might find this interesting") with links or attachments even from a known person. Call to ask whether they sent it
- Only trust security warnings coming directly from CPCS IT
- Don't open links or attachments when it is strange that the person sent this type of message
- Be skeptical of all emails and web sites you visit
- Do not use your CPCS email address for personal purposes
- The minute you think you are infected or clicked a bad link, shut down your PC and contact IT

Tip Sheet. Print this out for reference.

Social Engineering Red Flags

FROM

- I don't recognize the sender's email address as someone I **ordinarily communicate with**.
- This email is from **someone outside my organization and it's not related to my job responsibilities**.
- This email was sent from **someone inside the organization** or from a customer, vendor, or partner and is **very unusual or out of character**.
- Is the sender's email address from a **suspicious domain** (like micorsoft-support.com)?
- I **don't know the sender personally** and they **were not vouched for** by someone I trust.
- I **don't have a business relationship** nor any past communications with the sender.
- This is an **unexpected or unusual email** with an **embedded hyperlink or an attachment** from someone I haven't communicated with recently.

TO

- I was cc'd on an email sent to one or more people, but I **don't personally know** the other people it was sent to.
- I received an email that was also sent to an **unusual mix of people**. For instance, it might be sent to a random group of people at my organization whose last names start with the same letter, or a whole list of unrelated addresses.

HYPERLINKS

- I hover my mouse over a hyperlink that's displayed in the email message, but the **link-to address is for a different website**. (This is a **big red flag**.)
- I received an email that only has **long hyperlinks with no further information**, and the rest of the email is completely blank.
- I received an email with a **hyperlink that is a misspelling** of a known web site. For instance, www.bankofamerica.com — the "m" is really two characters — "r" and "n."



DATE

- Did I receive an email that I normally would get during regular business hours, but it was **sent at an unusual time** like 3 a.m.?

SUBJECT

- Did I get an email with a subject line that is **irrelevant or does not match** the message content?
- Is the email message a reply to something I **never sent or requested**?

ATTACHMENTS

- The sender included an email attachment that I **was not expecting** or that **makes no sense** in relation to the email message. (This sender doesn't ordinarily send me this type of attachment.)
- I see an attachment with a possibly **dangerous file type**. The only file type that is **always safe to click on is a .txt file**.

CONTENT

- Is the sender asking me to click on a link or open an attachment to **avoid a negative consequence** or to **gain something of value**?
- Is the email **out of the ordinary**, or does it have **bad grammar** or **spelling errors**?
- Is the sender asking me to click a link or open up an attachment that **seems odd or illogical**?
- Do I have an **uncomfortable gut feeling** about the sender's request to open an attachment or click a link?
- Is the email asking me to look at a **compromising or embarrassing picture** of myself or someone I know?

© 2018 KnowBe4, Inc. All rights reserved. Other product and company names mentioned herein may be trademarks and/or registered trademarks of their respective companies.

KnowBe4
Human error. Conquered.

Remotely accessing your PC (GoToMyPC)

GoToMyPC lets you remotely access your CPCS PC from another computer (home PC) or mobile device (smartphone, tablet). It lets you work on your CPCS PC from anywhere as if you are in the office. If your PC is on, GoToMyPC gives you access to all your files, network, tools, etc. that you have in the office.

GoToMyPC should be on your computer by default (you can find it under the Start Menu→Programs→GoToMyPC). If not, contact the helpdesk. Once installed, your PC must be on and logged in for it to work (it can be locked).

To use GoToMyPC from your phone or tablet, you must download the app from the app store.

Using GoToMyPC

You may access your work PC remotely by logging in to <https://www.gotomypc.com> or by using the app on your mobile phone or tablet.

You **MUST** leave your PC turned on at all times to be able to use GoToMyPC. It can be locked, but you must be logged in.

- Your GoToMyPC username will be your FULL email address
- You will need to supply a GoToMyPC password and Access Code. The GoToMyPC password will not change when you change your Windows password. **This password MUST be different from your CPCS login password.** The Access Code is a second password you'll be asked to create when logging into GoToMyPC. **This password MUST be different from your CPCS login password**

User guide is on the intranet under the "IT Resources" link or at https://www.gotomypc.com/downloads/pdf/p/GoToMyPC_Corporate_User_Guide.pdf.

Useful FAQs on GoToMyPC are under IT Resources in the intranet.

WiFi

Currently WiFi only supports access to the internet for connected devices. In late 2021 or early 2022 we will restore WiFi access for the intranet and network storage. This will be announced.

When in the office, look for the WiFi network **CPCS Guest**. The password for this is **Icecreamsandwich**.

Since this is a guest WiFi, the password may be shared with non-CPCS staff.

Case management

Zelly

Zelly is the CPCS unified case management system. It replaces three legacy systems. It is for all divisions.

For questions/help:

- zelly@publiccounsel.net.
- Do not contact the Help Desk.

Where to go for Zelly support:

- **40 training videos** (on Google Drive).
 - <https://drive.google.com/drive/u/2/folders/1LsP0gdogkIIYyx01P5GstT3tS0cMDXrW>
 - Most are under 5 minutes (see a listing at the end of the email)
- **User guide.**
 - <https://intranet.publiccounsel.net/it/zelly/> or at the information icon in Zelly
- **Information icon in Zelly.** Including frequently asked questions, user guide, training videos, definitions, icon descriptions, etc.
- **Intranet (internal web site).** Including frequently asked questions, user guide, training videos.
 - <https://intranet.publiccounsel.net/it/zelly/>
 - Internal web site accessed over GoToMyPC or when in the office

Legacy Systems

CPCS has three **legacy** case management systems for use by staff. They are only for references purposes and will be retired at the end of 2022.

The case management systems can be accessed internally or externally. They are:

CASEY

- For the **Criminal Division/Mental Health Division**
- <https://www.cpcsweb.net/casey/Login.aspx>
- For help contact casey@publiccounsel.net

TRIS

- For the **Youth Advocacy Division**
- <https://cpcs.publiccounsel.net/yad/>
- For help contact tris-cms@publiccounsel.net

CMS

- For the **Children and Family Law Division**
- <https://cpcs.publiccounsel.net/CAFL/>
- For help contact tris-cms@publiccounsel.net

Shared Laptops– Logging in

- The first time you use a shared laptop, you must plug it into the network, and then login. If you don't do this, you will be unable to login to the laptop
- If you haven't used a laptop in a while, plug it in to the network and try logging in before you leave the office to ensure everything is still working
- If you have changed your password since the last time you logged in, plug the laptop into the network and then login in with your new password.

Free conference calling

Sometimes we need to have a meeting with multiple staff members at different locations or even with people outside the CPCS organization. There are many technical solutions for this (Vsee for video conferencing, Skype, Google chat, Google + group chat, etc.), but the simplest, easiest, lowest technology approach is a traditional teleconference. Teleconferences are great because everyone knows how to use a phone, and it requires no installation of software on a device, no training, etc.

There are a number of free teleconferencing services that can be used. The two chief services used at CPCS are www.freeconferencecalling.com, because it is simple and www.freeconference.com, which is a bit more complex.

A caution for all these services is that they don't provide toll-free dialing or local phone numbers.

Listserv Access

IT has nothing to do with the listservs.

Listservs are online forums hosted by CPCS that allow communication between private counsel and staff. If a person needs to be added to a Listserv, there are different responsible parties depending on the practice area:

- **Adult criminal, murder, and juvenile listservs, as well as the PDD listserv** – Training Department (Karen Smolar)
- **Mental health** – MHLD (Mark Larsen)
- **SORB** – SRCSU (Pasqua Scibelli)
- **CAFL** – NONE – They do not use listservs