SIGNING UP FOR ACCOUNTS ONLINE

DITCHING YOUR MONITORED DEVICE

1. **FIND A DEVICE** that the perpetrator can't physically access—like a Palomar computer.
2. **SET UP A NEW EMAIL** account through gmail.com.
3. **NEVER CHECK IT** from your own computer or phone.
4. **ADD FILES** you want to keep safe to the Google Drive through this account.
5. **LOG OUT** when you have finished.

CREATING SAFE PROFILES

1. **DON'T USE IDENTIFYING INFORMATION** like your name or birth date in user names.
2. **USE DIFFERENT PROFILE PICTURES** and usernames for each site.
3. **ADD A PICTURE** that isn't of you for profile photos.
4. **DON'T SHARE PERSONAL INFORMATION** beyond what's necessary to create an account or profile.
5. **CHECK "NO"** if a site or app requests access to your contact list.
6. **OPT OUT** of the option to include your profile in site search results.

CREATING SECURE PASSWORDS

Secure passwords are long (12+ characters), mix letters with numbers and symbols, and include no personal information or dictionary words.

Use a phrase and incorporate shortcut codes or acronyms:

4Score&7yrsAgo (Four score and seven years ago)

Use passwords with common elements, but customized to specific sites:

Pwrd4Acct-$$ (Password for account at the bank)

Pwrd4Acct-FB (Password for a Facebook account)

Don't write passwords down or reuse them.

Select "no" when asked if you want the device, browser, site, or app to remember your password.

Use commonly allowed symbols:

! " # $ % & ' ( ) * + , - . / : ; < = > ? [\ ] ^ _ { | } ` ~

Use basic smiley faces:

:) =) :< :s ;) :3 :L :D :] :} :o :/ <3

Palomar
OKLAHOMA CITY'S FAMILY JUSTICE CENTER

A PROJECT WITH THE CITY OF OKLAHOMA CITY

1140 N. Hudson Ave, Oklahoma City, OK 73103
405.552.1010 | www.palomarokc.org
Ask for Bekah for tech help.

SIGNING UP FOR ACCOUNTS ONLINE

ENABLING TWO-FACTOR AUTHENTICATION

Adding Two Factor Authentication to your accounts gives them an extra layer of security by requiring, in addition to a password and username, something that only you would have.

USING USB SECURITY KEYS

Some sites support the use of a physical USB security key as a second authentication factor. Rather than receiving a code to enter, you would insert the USB when prompted. Inexpensive versions can be purchased online.

Check your existing email accounts to make sure that your messages have not been forwarded without your knowledge.

ADDING TWO-FACTOR AUTHENTICATION TO YOUR ACCOUNTS

Google	My Account > Sign-in & Security > 2-Step Verification
Microsoft	Microsoft account > Security > More Security Options > Set up two-step verification
YAHOO!	Account Security > Two-Step Verification
facebook	Settings > Security > Two-Factor Authentication
Apple	My Apple ID page > Security > Two-Factor Authentication

BANKING ONLINE

To avoid having your paper statements stolen, enroll in online banking and choose to receive digital statements. Sign out and close the browser window when you have finished viewing your account. Select security questions that only you are able to answer. If the perpetrator likely knows your personal details, substitute different answers to the regular questions. For example, your answer to "What is your mother's maiden name?" might instead be your mother's favorite food. Memorize your PINs and passwords.

Palomar
OKLAHOMA CITY'S FAMILY JUSTICE CENTER

A PROJECT WITH THE CITY OF OKLAHOMA CITY

1140 N. Hudson Ave, Oklahoma City, OK 73103
405.552.1010 | www.palomarokc.org
Ask for Bekah for tech help.