PCGenesis: Ransomware Attacks and Backing up PCGenesis

- GASBO
- Augusta, GA
- November 8, 2023

Agenda

- Ransomware Attacks
- Backing Up PCGenesis

Ransomware

What is ransomware?

Ransom malware, or ransomware, is a type of malware that prevents users from accessing their system or personal files and demands ransom payment in order to regain access.

Encrypting Ransomware

This is the one we have been seeing in our districts. The perpetrators snatch up your files and encrypt them, demanding payment in order to decrypt and redeliver. The reason why this type of ransomware is so dangerous is because once cybercriminals get ahold of your files, no security software or system restore can return them to you.

Unless you contact the cybercriminals and pay the ransom, they're gone. Even if you pay them, there is no guarantee will give you those files back.

Who do ransomware authors target?

When ransomware was first unleashed, its initial victims were sent to the general public.

However, they began to realize its full potential when they rolled out ransomware to businesses and now public institutions, such as school districts. Multiple Georgia districts have already been hit.

How do you get infected with Ransomware?

- Email

The most common method today is through malicious spam email. The email might contain booby-trapped attachments, such as PDFs or Word documents or links to malicious websites.

Other ways of being infected with Malware

Transferred from connected devices

If Windows malware is on the smartphone, you plug it into your computer, and autorun is running, the Windows-based malware could start running and infect your machine.

Do not charge your devices using your USB port.

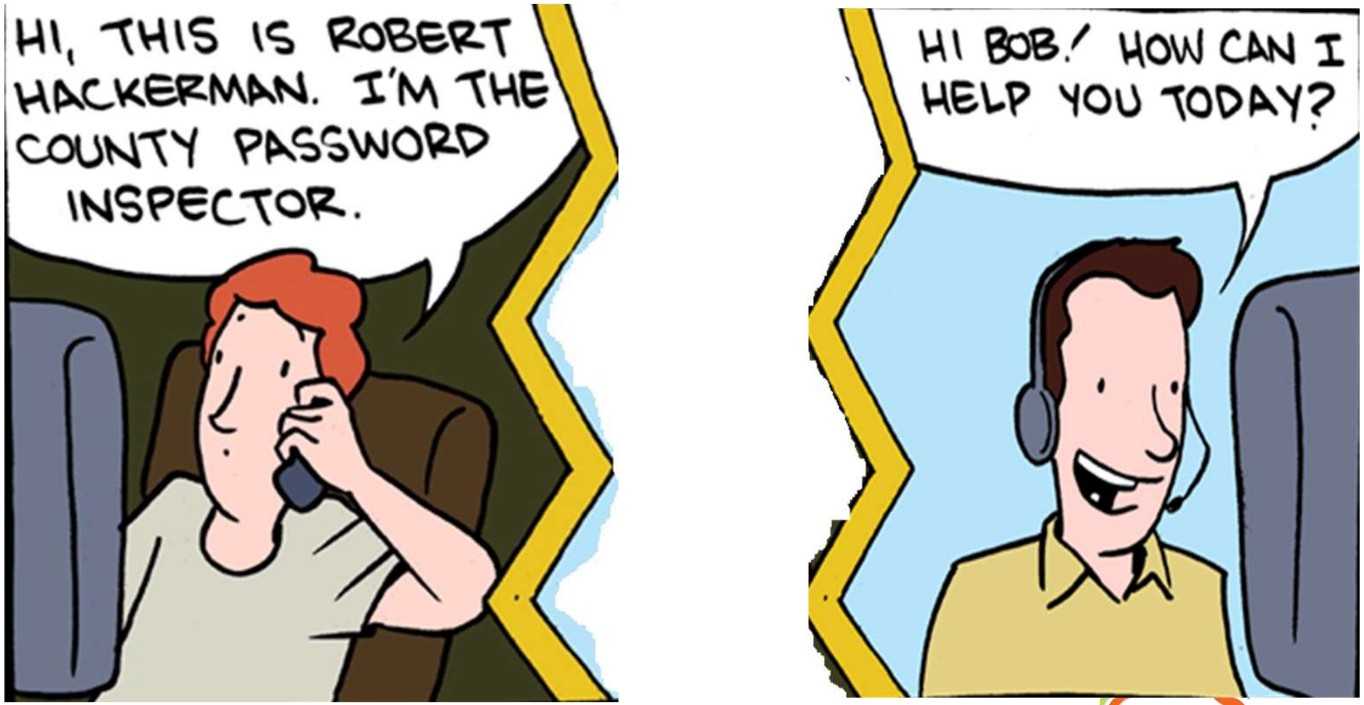
Other ways of getting infected

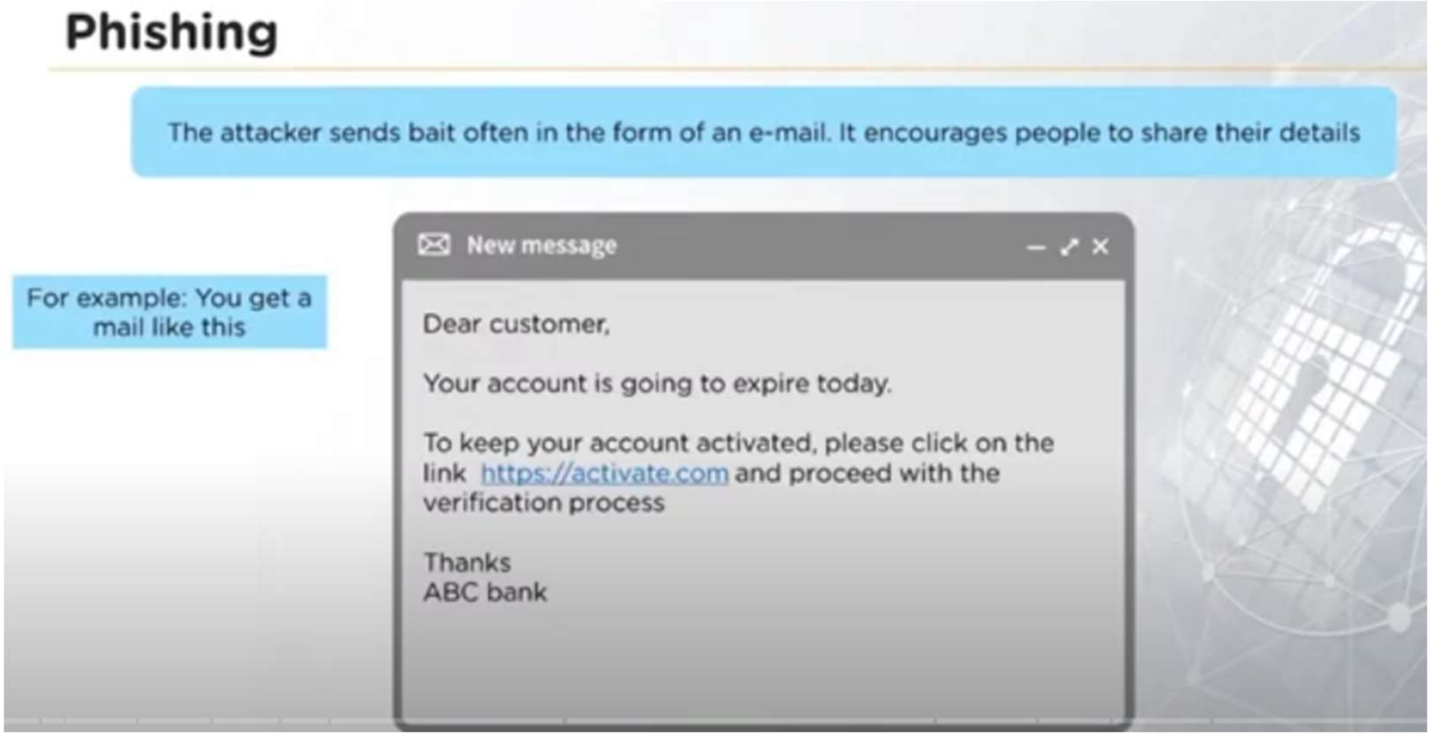
Accidental sharing with a thief

“Movie Hacker”

IF I CAN JUST OVERCLOCK THE UNIX DJANGO, I CAN BASIC THE DDOS ROOT. NO DICE. BUT WAIT... IF I DISENCRYPT THEIR KILOBYTES WITH A BACKDOOR HANDSHAKE THEN... JACKPOT.

Real Hacking


HI, THIS IS ROBERT HACKERMAN. I'M THE COUNTY PASSWORD INSPECTOR.
HI BOB! HOW CAN I HELP YOU TODAY?



Phishing

The attacker sends bait often in the form of an e-mail. It encourages people to share their details

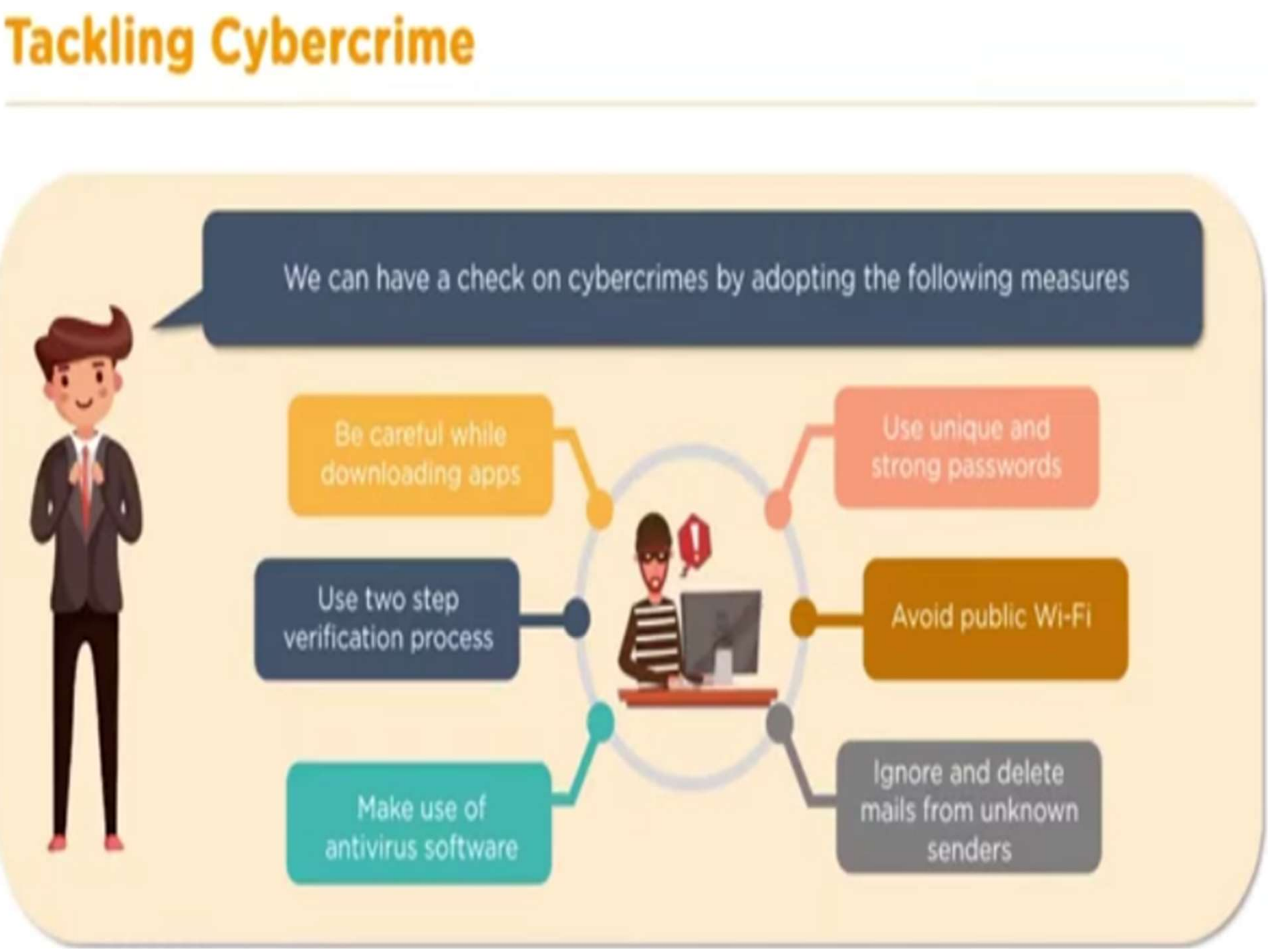
For example: You get a mail like this

Dear customer,

Your account is going to expire today.

To keep your account activated, please click on the link https://activate.com and proceed with the verification process

Thanks
ABC bank



Tackling Cybercrime

We can have a check on cybercrimes by adopting the following measures

- Be careful while downloading apps
- Use two step verification process
- Make use of antivirus software
- Use unique and strong passwords
- Avoid public Wi-Fi
- Ignore and delete mails from unknown senders

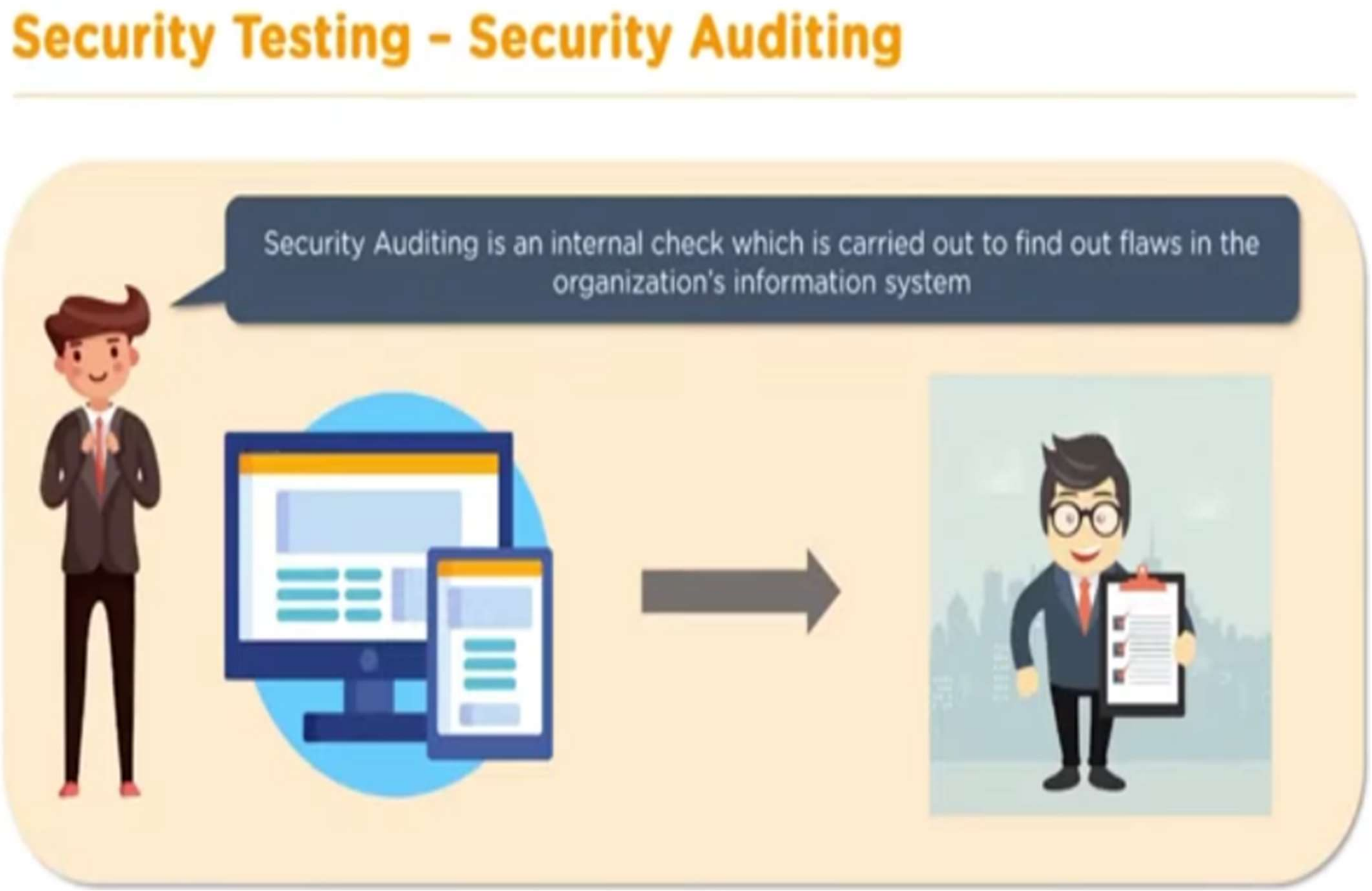
How to protect from ransomware

- Create secure daily backups of your PCGenesis data to a new thumb drive and label with date and time.

- Invest in cybersecurity—a program with real-time protection that's designed to thwart advanced malware attacks such as ransomware. You should also look out for features that will both shield vulnerable programs from threats (an anti-exploit technology) as well as block ransomware from holding files hostage (an anti-ransomware component).

  Be sure your systems and software are updated. The WannaCry ransomware outbreak took advantage of a vulnerability in Microsoft software. While the company had released a patch for the security loophole back in March 2017, many folks didn't install the update—which left them open to attack.

  - We recommend changing your settings to enable automatic updating.

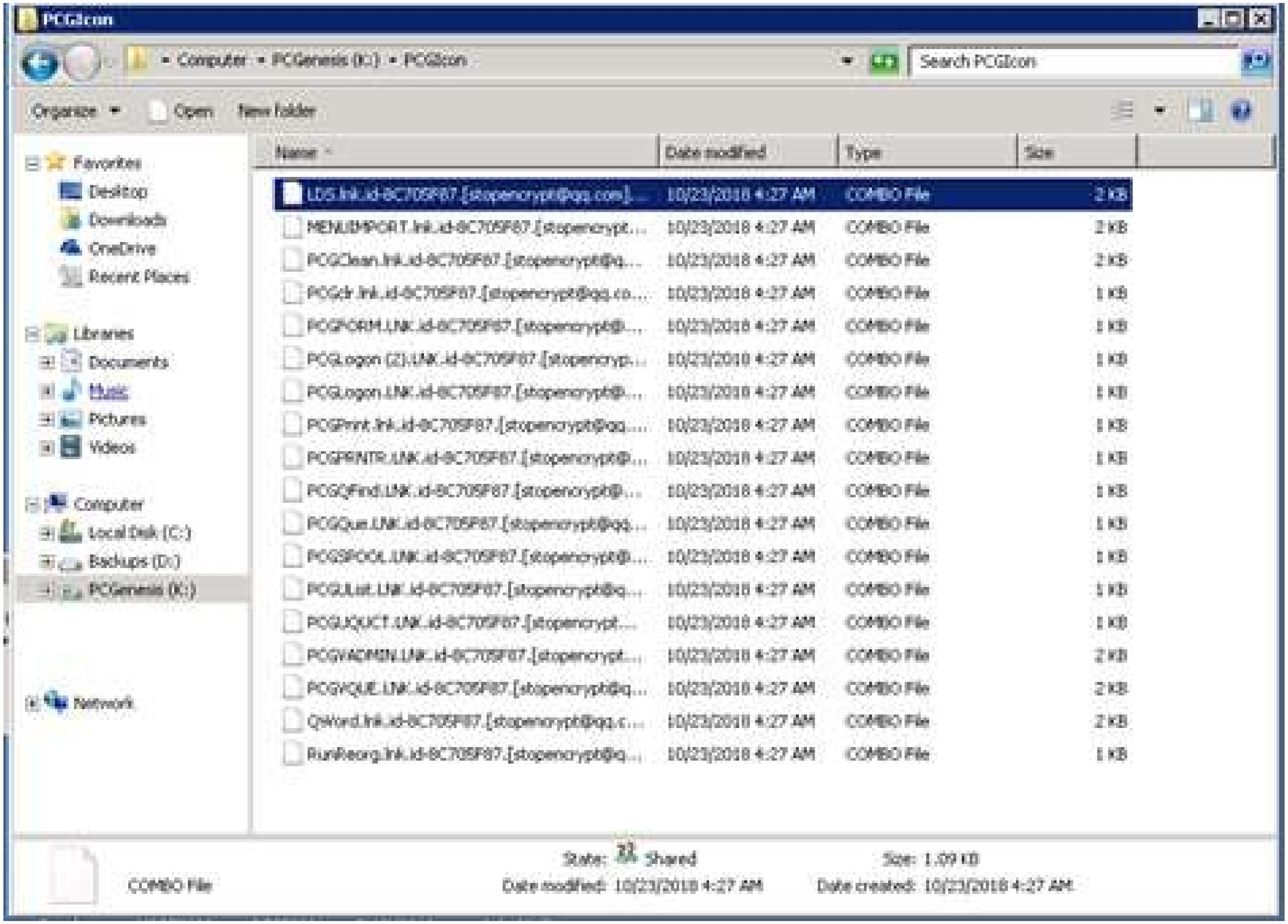


Security Testing - Security Auditing

Security Auditing is an internal check which is carried out to find out flaws in the organization's information system

How do you know if you have been infected?

Filenames will all be changed, nothing works and everything you click sends you to a website announcing to fix your files for a fee.



Name	Date modified	Type	Size
LDS.lnk.id-8C705F87.[stopencrypt@qq.com]...	10/23/2018 4:27 AM	COMBO File	2 KB
MENUIMPORT.lnk.id-8C705F87.[stopencrypt...	10/23/2018 4:27 AM	COMBO File	2 KB
PCGClean.lnk.id-8C705F87.[stopencrypt@q...	10/23/2018 4:27 AM	COMBO File	2 KB
PCGclr.lnk.id-8C705F87.[stopencrypt@qq.co...	10/23/2018 4:27 AM	COMBO File	1 KB
PCGFORM.LNK.id-8C705F87.[stopencrypt@...	10/23/2018 4:27 AM	COMBO File	1 KB
PCGLogon (2).LNK.id-8C705F87.[stopencryp...	10/23/2018 4:27 AM	COMBO File	1 KB
PCGLogon.LNK.id-8C705F87.[stopencrypt@...	10/23/2018 4:27 AM	COMBO File	1 KB
PCGPrint.lnk.id-8C705F87.[stopencrypt@qq....	10/23/2018 4:27 AM	COMBO File	1 KB
PCGPRINTR.LNK.id-8C705F87.[stopencrypt@...	10/23/2018 4:27 AM	COMBO File	1 KB
PCGQFind.LNK.id-8C705F87.[stopencrypt@...	10/23/2018 4:27 AM	COMBO File	1 KB
PCGQue.LNK.id-8C705F87.[stopencrypt@qq...	10/23/2018 4:27 AM	COMBO File	1 KB
PCGSPOOL.LNK.id-8C705F87.[stopencrypt@...	10/23/2018 4:27 AM	COMBO File	1 KB
PCGUList.LNK.id-8C705F87.[stopencrypt@q...	10/23/2018 4:27 AM	COMBO File	1 KB
PCGUQUCT.LNK.id-8C705F87.[stopencrypt....	10/23/2018 4:27 AM	COMBO File	1 KB
PCGVADMIN.LNK.id-8C705F87.[stopencrypt...	10/23/2018 4:27 AM	COMBO File	2 KB
PCGVQUE.LNK.id-8C705F87.[stopencrypt@q...	10/23/2018 4:27 AM	COMBO File	2 KB
QWord.lnk.id-8C705F87.[stopencrypt@qq.c...	10/23/2018 4:27 AM	COMBO File	2 KB
RunReorg.lnk.id-8C705F87.[stopencrypt@q...	10/23/2018 4:27 AM	COMBO File	1 KB

COMBO File

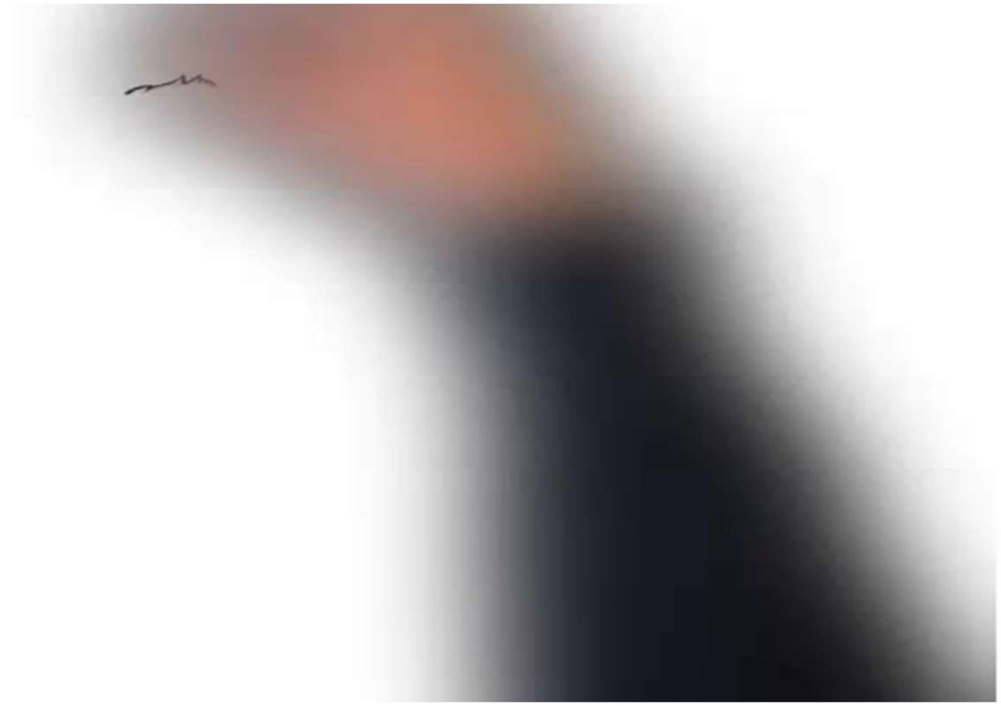
State: Shared

Size: 1.09 KB

Date modified: 10/23/2018 4:27 AM

Date created: 10/23/2018 4:27 AM

What NOT to do if infected!



The number one rule if you find yourself infected with ransomware is to **never pay the ransom**.

(This is now advice endorsed by the FBI.)

Nothing on a computer exposed to ransomware can be trusted. The computer must be completely reformatted.

How to recover from a ransomware attack?

- Due to multiple attacks, we now can advise districts on streamlining the recovery effort.

- If you see your PCGicon folder files looking distorted, you have been infected. The entire PCGenesis server has been compromised and must be reformatted. Nothing on this server should be trusted.

- Please contact the DOE immediately for instructions on moving forward in the event of a ransomware attack.

What is the FIRST question the DOE help desk will ask?

“Do you have an offline or cloud **BACKUP** that is not located on the infected network”?

The ability to recover quickly depends on a non-infected backup.

Your exposure depends on how much work was done in PCG since the last backup of two folders **K:\PCGSQLdb and K\SECOND**.

Site Recommendations

- Weekly full system backup of **K:\*.*** (Retain 3 weeks)

- Daily backup of data (**K:\SECOND and K:\PCGSQLDB**) to CD/DVD/USB (Retain for 1 month)

Why Back up PCGenesis Data files?

To Limit Exposure from:

- 1) System hardware failure

- 2) Accidental Data Corruption

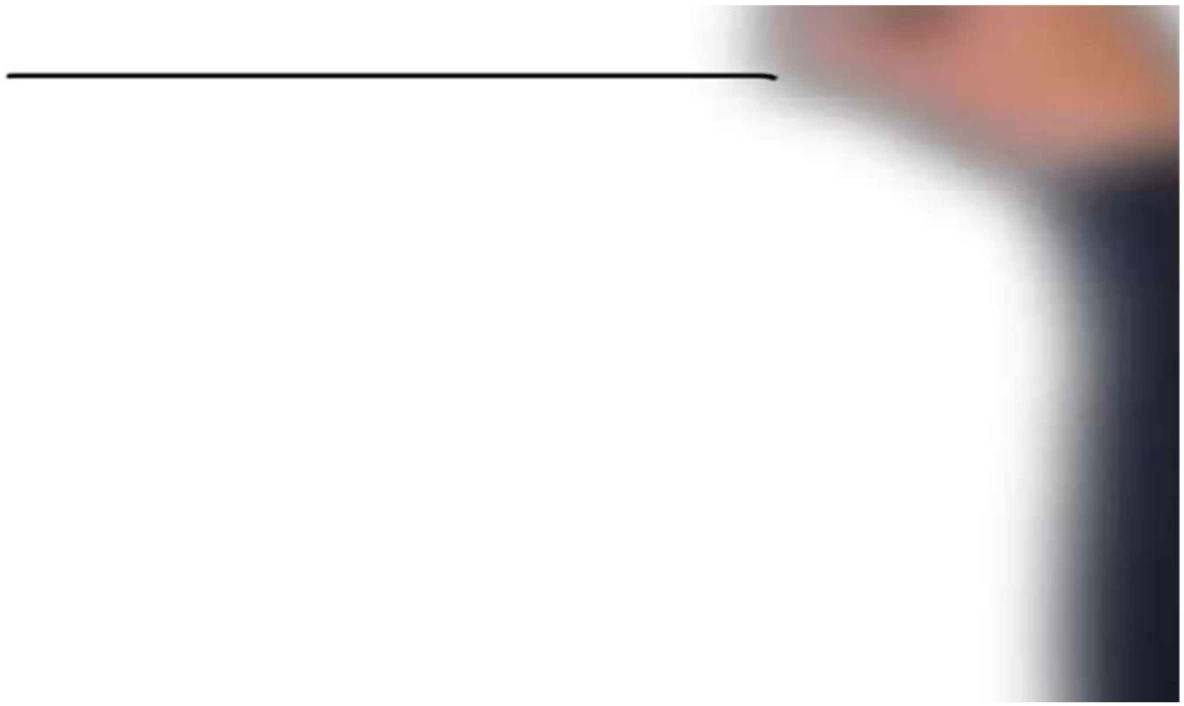
  - (someone overlayed with last year's data)

- 3) Purposeful Data corruption

  - (someone overlayed with last year's data)

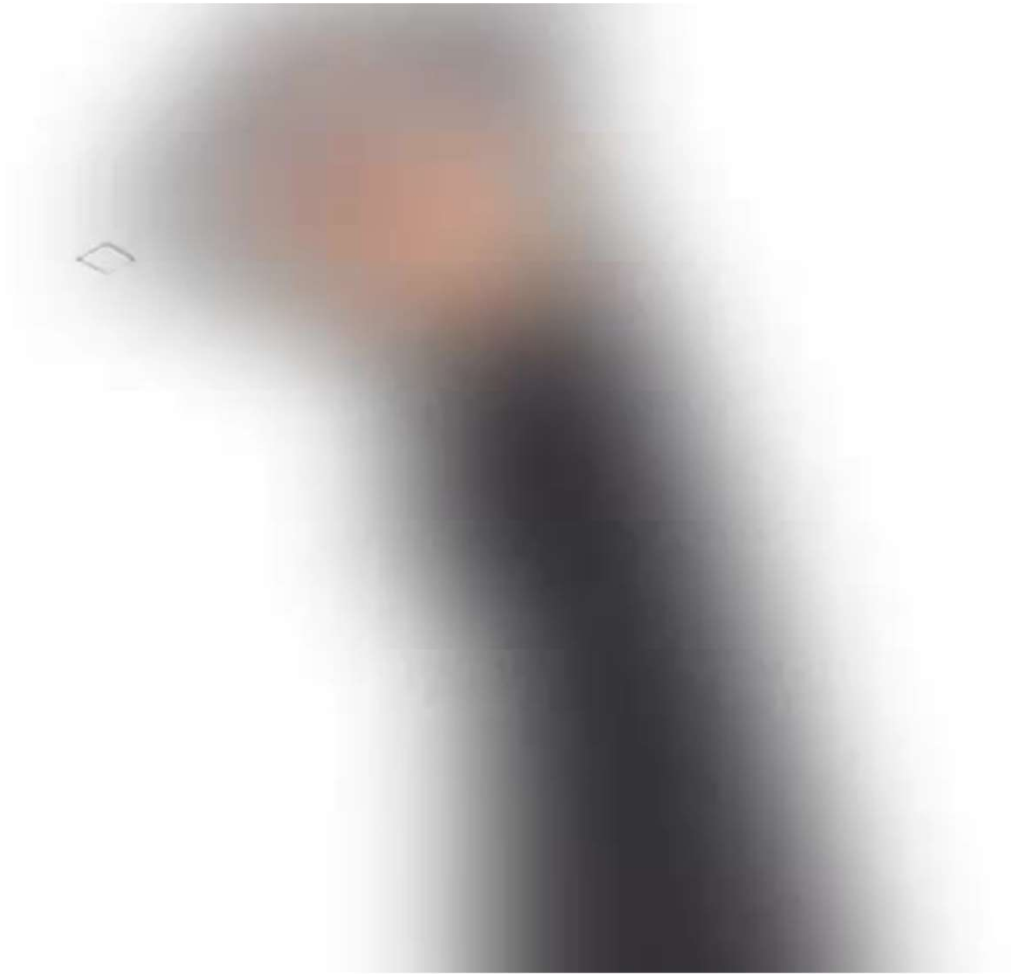
  - Virus or Ransomware attack

Where is PCGenesis data?



K:\SECOND	5%
K:\PCGSQLdb ⇐	95%

Where to Back up PCGenesis Data?



What files MUST be backed up?

It does absolutely no good if **K:\SECOND** is on the backup, but **K:\PCGSQLdb** is not!

- **K:\SECOND** cannot be restored without also restoring the **PCGenesisDB** database.
- These two entities must be kept in sync, otherwise financial and payroll postings may be lost

- All of your recent financial data is gone!
- All of your recent payroll data is gone!
- All of your recent CPI data is gone!

VERIFY that both files are being backed up

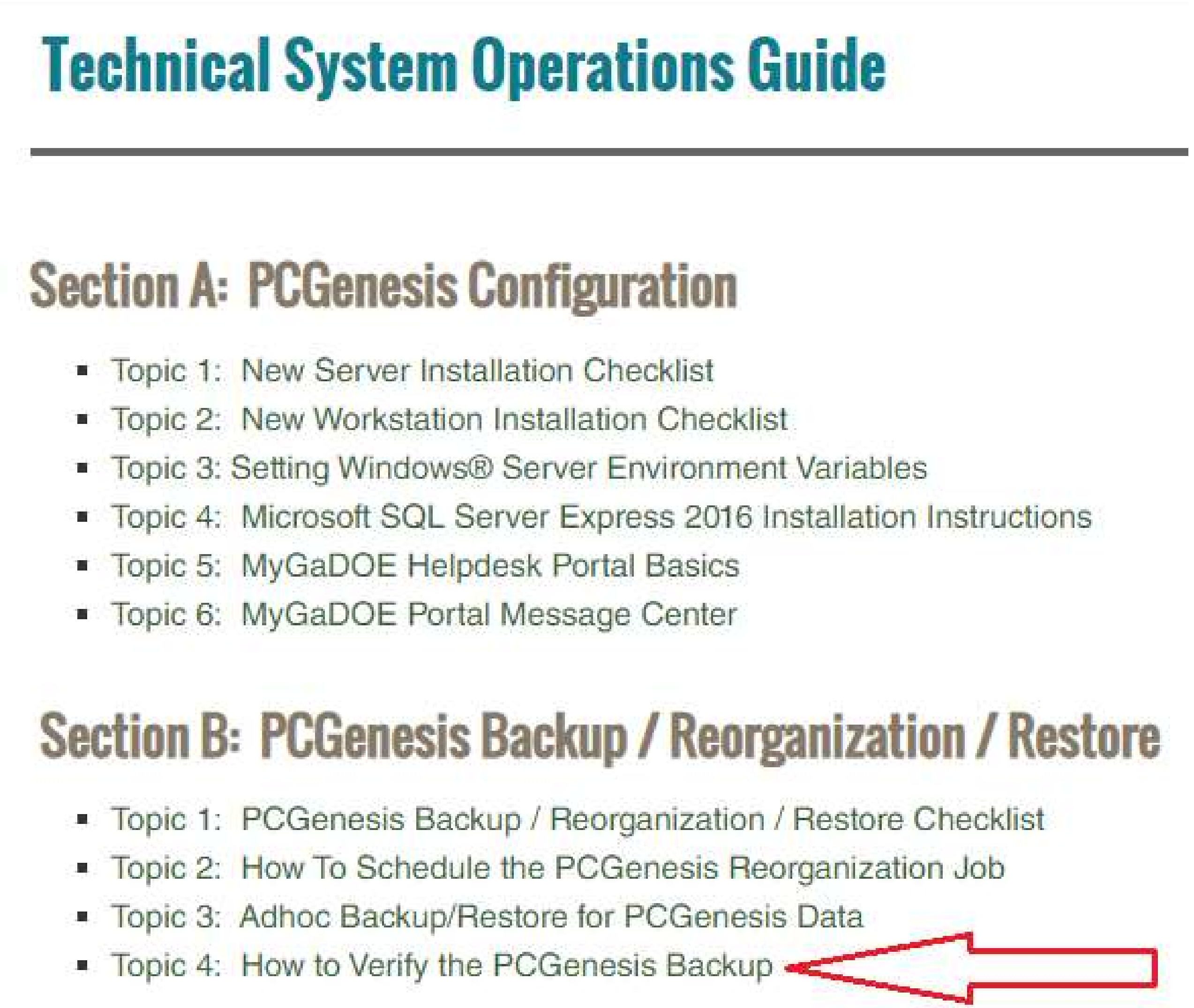
- The help desk has worked with multiple school districts that realize AFTER a ransomware attack that they were not getting **K:\PCGSQLdb** copied to a backup!

- This is all too common!

What if there is no K:\PCGSQLdb backup?

- It has taken everybody involved hours, days, and weeks to recover data.
- Is payroll going to be ready in time if you have to recover?!

Ransomware Attacks and Backing Up PCGenesis



Technical System Operations Guide

Section A: PCGenesis Configuration

- Topic 1: New Server Installation Checklist
- Topic 2: New Workstation Installation Checklist
- Topic 3: Setting Windows® Server Environment Variables
- Topic 4: Microsoft SQL Server Express 2016 Installation Instructions
- Topic 5: MyGaDOE Helpdesk Portal Basics
- Topic 6: MyGaDOE Portal Message Center

Section B: PCGenesis Backup / Reorganization / Restore

- Topic 1: PCGenesis Backup / Reorganization / Restore Checklist
- Topic 2: How To Schedule the PCGenesis Reorganization Job
- Topic 3: Adhoc Backup/Restore for PCGenesis Data
- Topic 4: How to Verify the PCGenesis Backup

All you need for a disaster recovery:

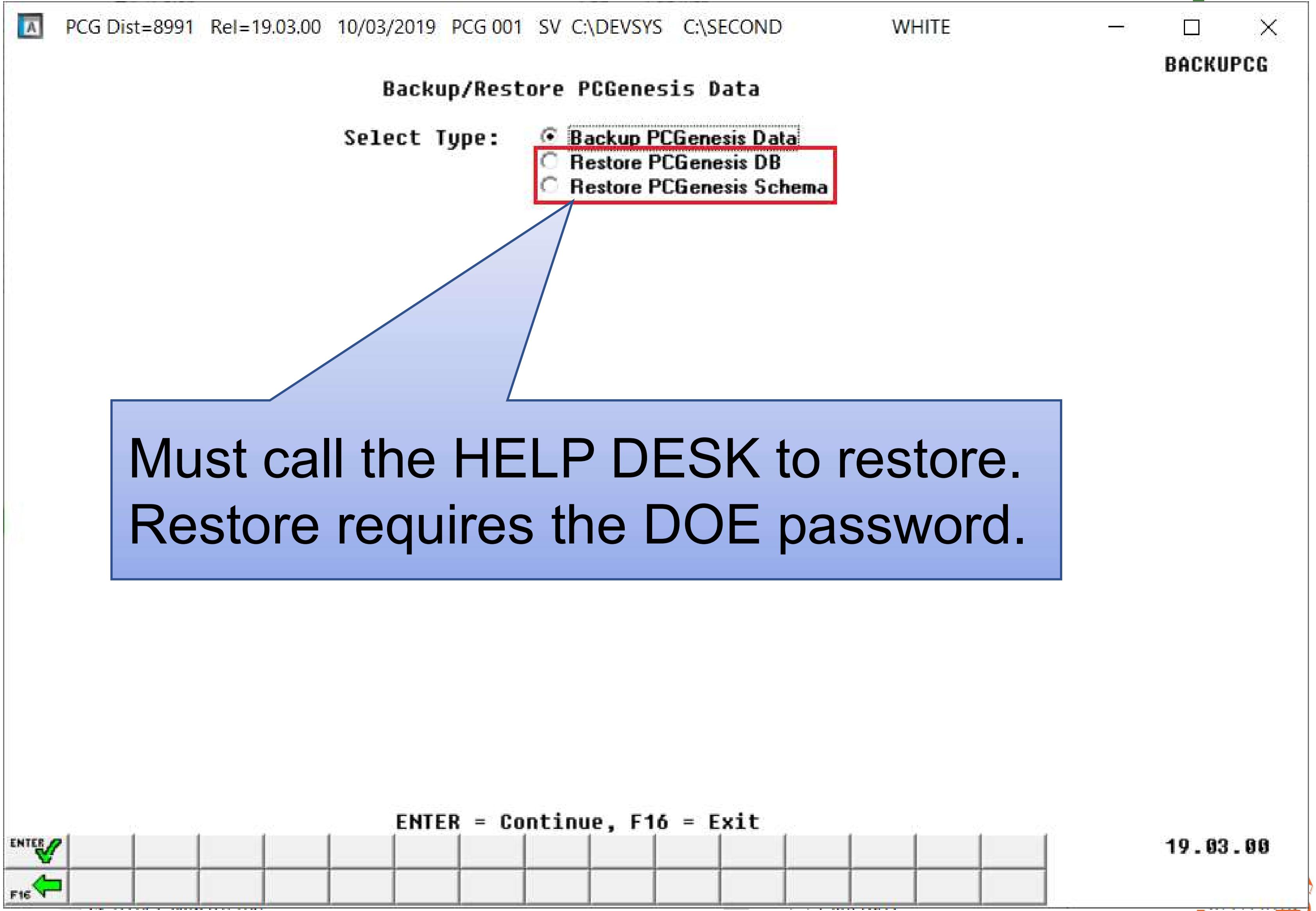
- K:\PCGSQLdb
- K:\SECOND

Make your IT department **VERIFY** Verify that these two directories are on your backup media.

Adhoc Backup/Restore Option for PCGenesis Data

- On the ***System Utilities Menu***
- ***Backup / Restore PCGenesis Data*** (F30, F12).
- This is a quick and easy way to get a backup!
- Backs up the important PCGenesis data.

PCGenesis Databases - Backup



PCG Dist=8991 Rel=19.03.00 10/03/2019 PCG 001 SV C:\DEVSYS C:\SECOND WHITE

BACKUPCG

Backup/Restore PCGenesis Data

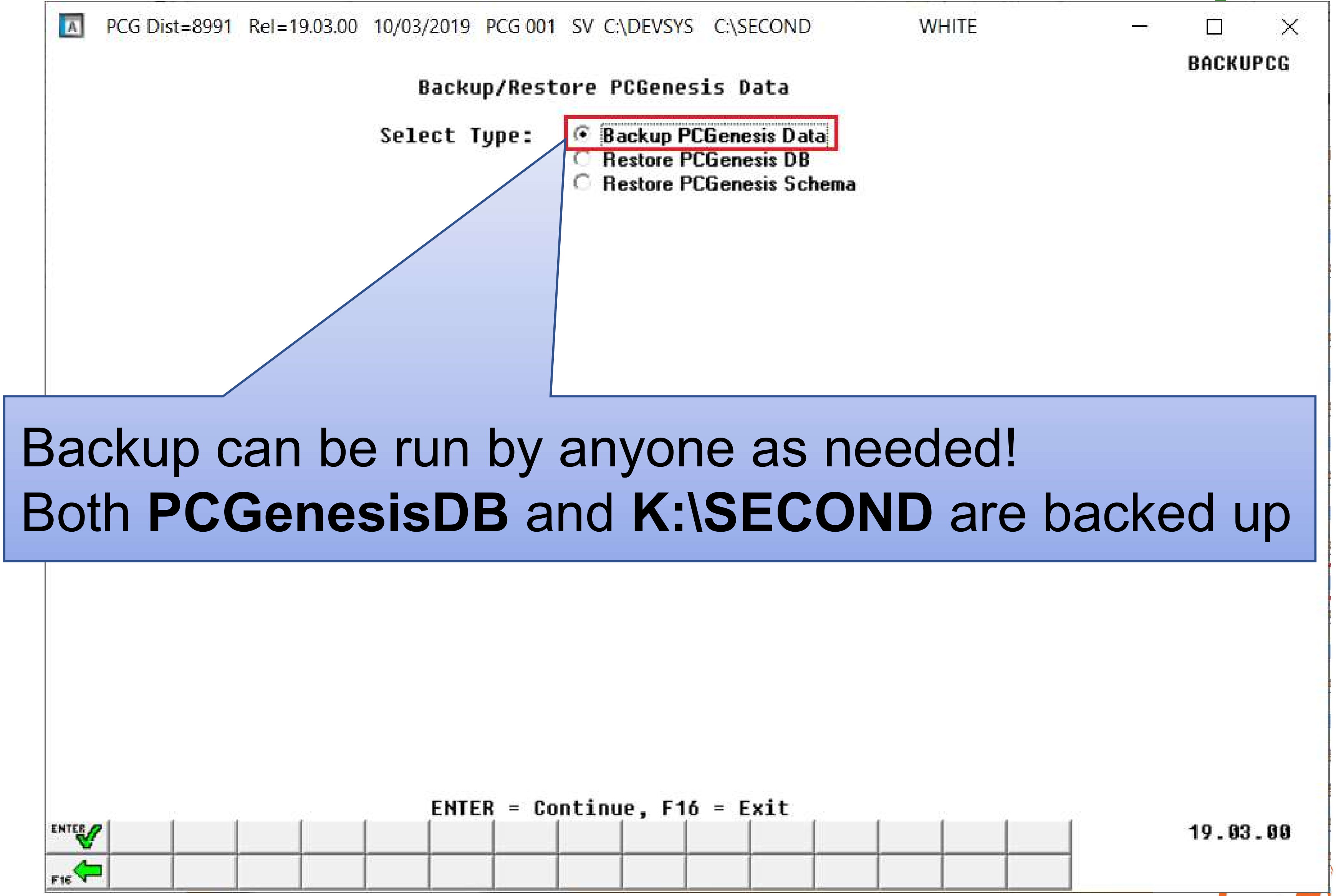
Select Type: ● Backup PCGenesis Data
○ Restore PCGenesis DB
○ Restore PCGenesis Schema

Must call the HELP DESK to restore.
Restore requires the DOE password.

ENTER = Continue, F16 = Exit

19.03.00

PCGenesis Databases - Backup



PCG Dist=8991 Rel=19.03.00 10/03/2019 PCG 001 SV C:\DEVSYS C:\SECOND WHITE

BACKUPCG

Backup/Restore PCGenesis Data

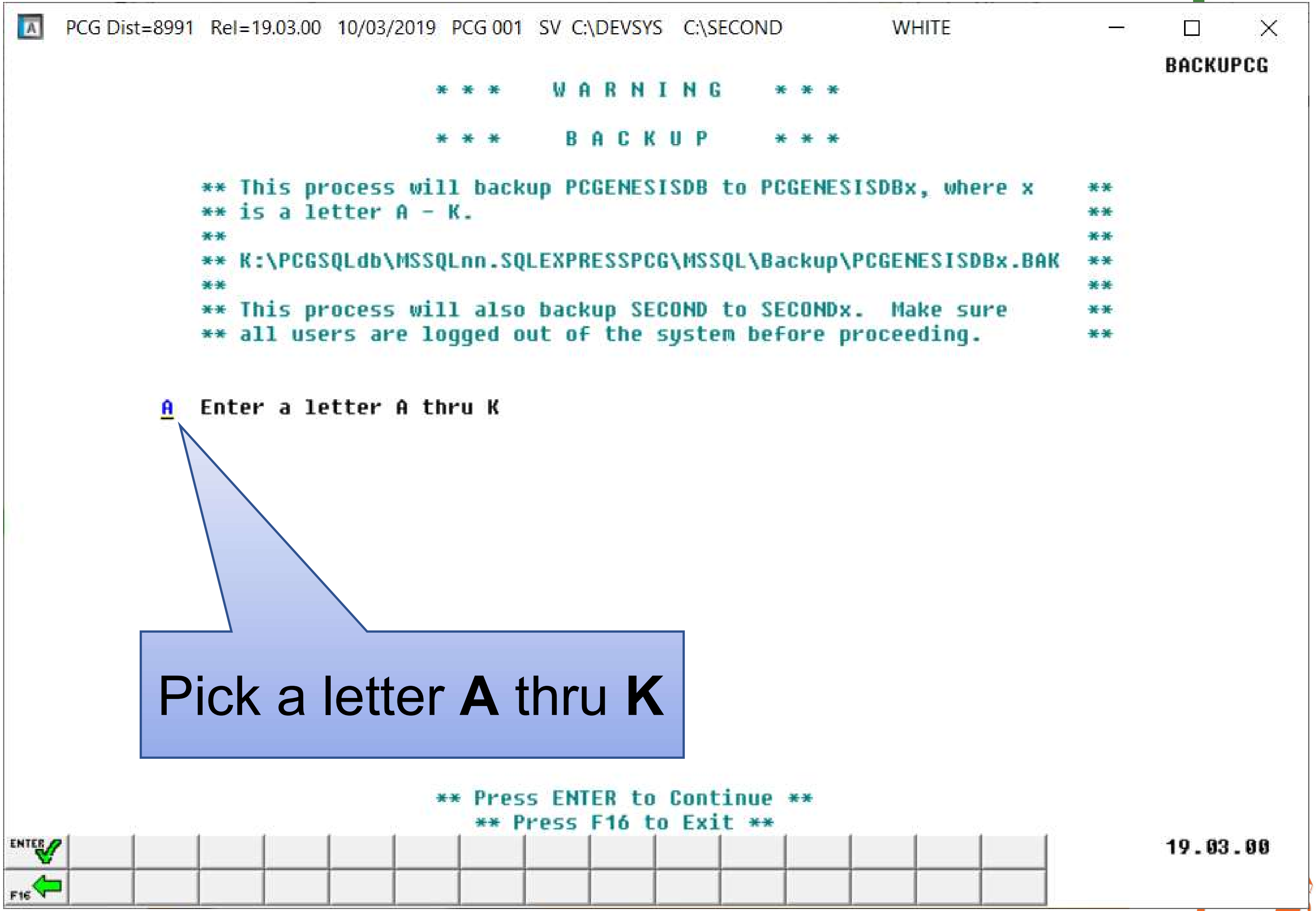
Select Type: ● Backup PCGenesis Data
○ Restore PCGenesis DB
○ Restore PCGenesis Schema

Backup can be run by anyone as needed!
Both **PCGenesisDB** and **K:\SECOND** are backed up

ENTER = Continue, F16 = Exit

19.03.00

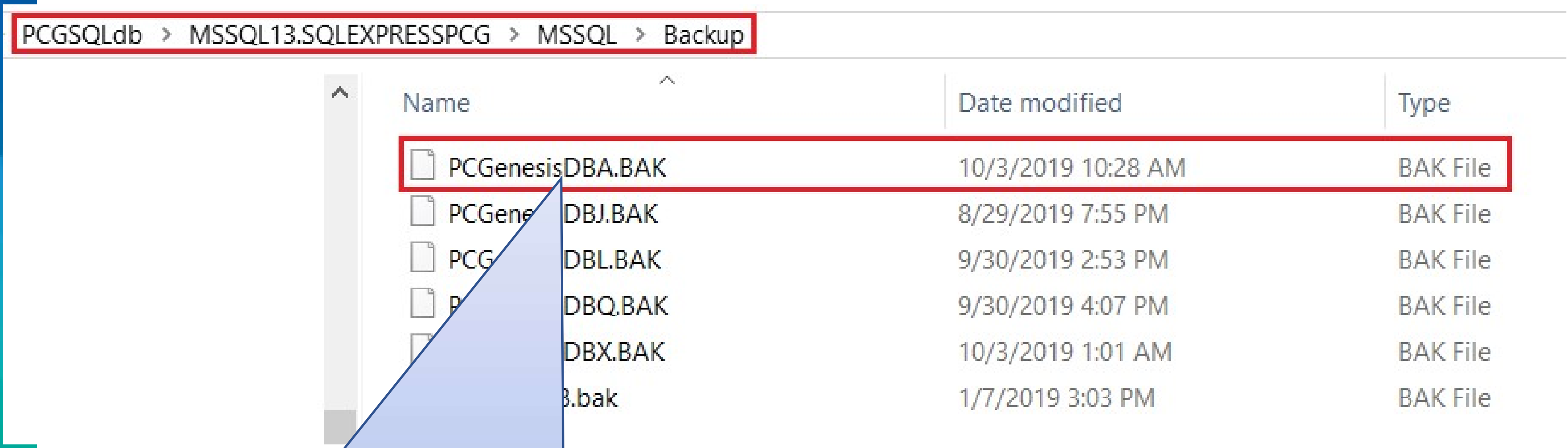
PCGenesis Databases - Backup



```
PCG Dist=8991   Rel=19.03.00   10/03/2019   PCG 001   SV  C:\DEVSYS   C:\SECOND          WHITE
                                                                                        BACKUPCG
                       * * *   W A R N I N G   * * *

                       * * *    B A C K U P    * * *

       ** This process will backup PCGENESISDB to PCGENESISDBx, where x    **
       ** is a letter A - K.                                                **
       **                                                                   **
       ** K:\PCGSQLdb\MSSQLnn.SQLEXPRESSPCG\MSSQL\Backup\PCGENESISDBx.BAK  **
       **                                                                   **
       ** This process will also backup SECOND to SECONDx.  Make sure      **
       ** all users are logged out of the system before proceeding.        **


     A  Enter a letter A thru K



                       ** Press ENTER to Continue **
                          ** Press F16 to Exit **
                                                                        19.03.00
```

Pick a letter **A** thru **K**

PCGenesis Databases - Backup



PCGSQLdb › MSSQL13.SQLEXPRESSPCG › MSSQL › Backup

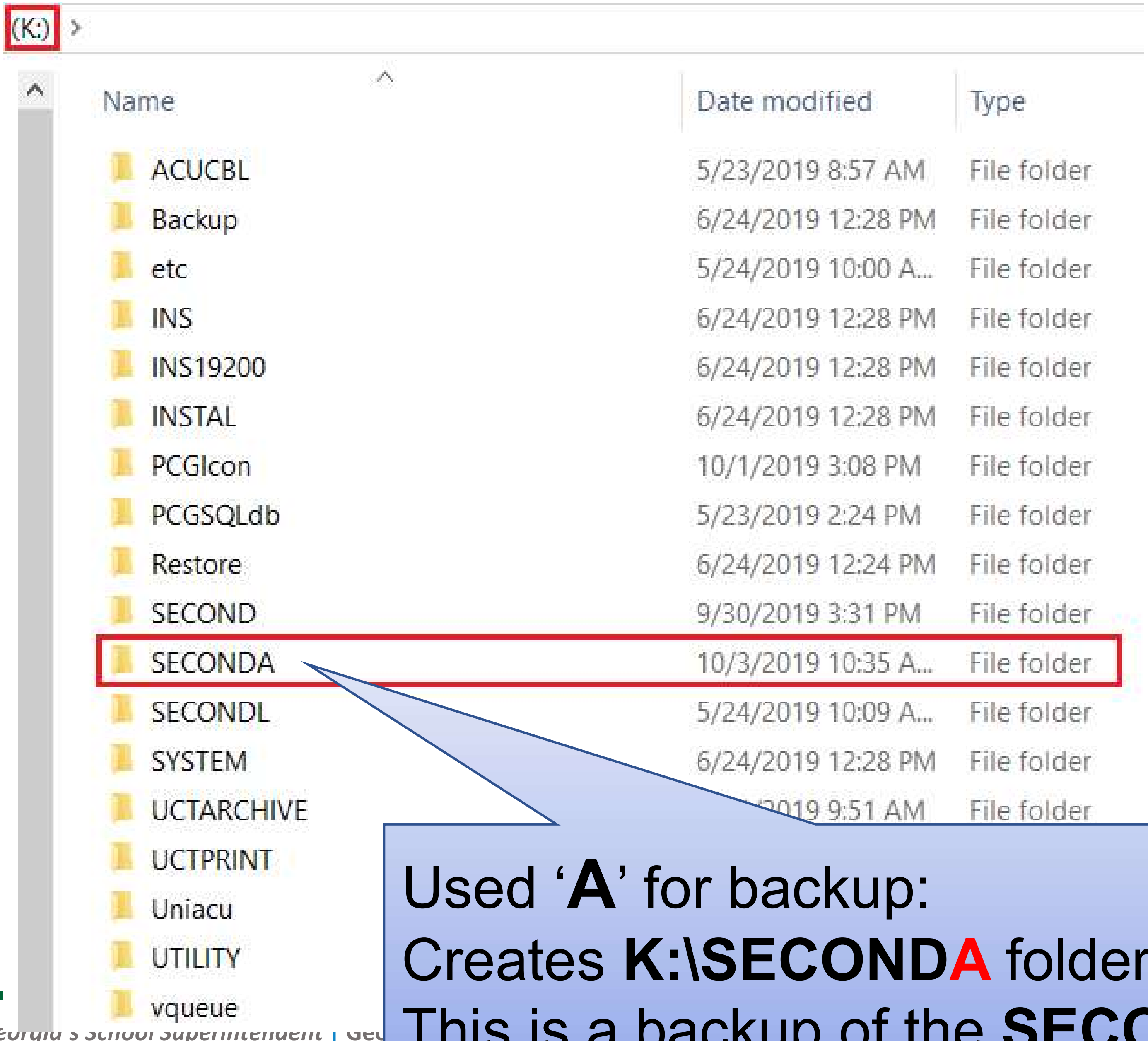
Name	Date modified	Type
PCGenesisDBA.BAK	10/3/2019 10:28 AM	BAK File
PCGene DBJ.BAK	8/29/2019 7:55 PM	BAK File
PCG DBL.BAK	9/30/2019 2:53 PM	BAK File
P DBQ.BAK	9/30/2019 4:07 PM	BAK File
DBX.BAK	10/3/2019 1:01 AM	BAK File
3.bak	1/7/2019 3:03 PM	BAK File

Used ‘**A**’ for backup:

Creates **PCGenesisDBA.BAK** in **Backup** folder

This is a backup of the database!

PCGenesis Databases - Backup



(K:) >

Name	Date modified	Type
ACUCBL	5/23/2019 8:57 AM	File folder
Backup	6/24/2019 12:28 PM	File folder
etc	5/24/2019 10:00 A...	File folder
INS	6/24/2019 12:28 PM	File folder
INS19200	6/24/2019 12:28 PM	File folder
INSTAL	6/24/2019 12:28 PM	File folder
PCGIcon	10/1/2019 3:08 PM	File folder
PCGSQLdb	5/23/2019 2:24 PM	File folder
Restore	6/24/2019 12:24 PM	File folder
SECOND	9/30/2019 3:31 PM	File folder
SECONDA	10/3/2019 10:35 A...	File folder
SECONDL	5/24/2019 10:09 A...	File folder
SYSTEM	6/24/2019 12:28 PM	File folder
UCTARCHIVE	2019 9:51 AM	File folder
UCTPRINT		
Uniacu		
UTILITY		
vqueue		

Used ‘**A**’ for backup:
Creates **K:\SECONDA** folder
This is a backup of the **SECOND** data!

PCGenesis Databases - Backup

Now *you* have control of your backup:

1. Zip K:\SECONDx → **SECONDx.zip**
2. Locate PCGenesisDBx.BAK in

   K:\PCGSQLdb\MSSQL13.SQLEXPRESSPCG\MSSQL\Backup
3. Copy PCGenesisDBx.BAK to root of K:
4. Zip K:\PCGenesisDBx.BAK → **PCGenesisDBx.BAK.zip**
5. Copy both zip files to USB drive
6. You have your own backup of your data!

PCGenesis Databases - Backup

If you put your backup on a small storage device like USB:

- Remember this backup contains sensitive payroll data
- Make sure to keep your storage device in a **secure location**!
- Don't store in desk drawers, pockets, backpacks, purses, etc.

Thank you for attending!