(membership includes monthly subscription)

The Digital VIKING

Twin Cities PC USER GROUP NEWSLETTER

Minneapolis & St. Paul, Minnesota USA • Vol. 46 No.8• March 2026

TC/PC Exists to Facilitate and Encourage the Cooperative Exchange of PC Knowledge and Information Across All Levels of Experience

March 2026

General Meeting

Tuesday, March 10, 2026

7:00 PM

Best of the CES 2026

Via Zoom Only

Once again we will watch a set of curated videos on YouTube where attendees at the Consumer Electronics Show (CES) in Las Vegas. Many videos were pre-screened and many rejected because all they focused on were robots, so many robots. The selection you will be watching are those that, for the most part, focused on products you might actually buy and use. Bring your popcorn!

Note: All TC/PC Meetings and SIG Groups will be virtual until further notice. Visit tcpc.com for info.

Tech Topics with Jack Ungerleider via Zoom at 6pm before the General Meeting.

The Digital Viking

The Digital Viking is the *official monthly publication of the Twin Cities PC User Group, a 501(c)(3)organization and an all-volunteer organization dedicated to users of IBM-compatible computers. Subscriptions are included in membership. We welcome articles and reviews from members.* The Digital Viking is a *copyrighted publication and reproduction of any material is expressly prohibited without permission. Exception: other User Groups may use material if unaltered and credited.*

Advertising

Full page (7½ x 9½)	**$100.00**
Two-thirds page (7½ x 6)	**80.00**
Half page (7½ x 4¾)	**65.00**
One-third page (7½ x 3)	**50.00**
Quarter page (3½ x 4¾)	**40.00**
Member Bus. Card (2 x 3½)	**10.00**

Multiple insertion discounts available.

Contact Sharon Walbran at:: SQWalbran@yahoo.com

Deadline for ad placement is the 1st of the month prior to publication. All rates are per issue and for digital or camera-ready ads. Typesetting and other services are extra and must be requested in advance of submission deadlines.

Payment must accompany order unless other arrangements are made in advance. Place make checks payable to: **Twin Cities PC User Group**

TC/PC 2025-2026 Board of Directors

Meets once or twice per year. All members welcome to attend.
Visit www.tcpc.com for meeting details.

President —Lee Kaphingst	leekap@comcast.net
Vice President —Curtiss Trout	ctrout@troutreach.com
Secretary - Sharon Walbran	sharon.walbran@gmail.com
Treasurer - Sharon Trout	strout@troutreach.com
Newsletter Publisher Sharon Walbran	952-925-2726 sharon.walbran@gmail.com
Web Master Curt Trout	ctrout@troutreach.com
Board Members:	
Steve Kuhlmey	skuhlmey@hotmail.com
Lon Ortner	612-824-4946 lon@csacomp.com
Lee Kaphingst	leekap@comcast.net
Jeannine Sloan	Ambassador for Friendship Village
Curtiss Trout	ctrout@troutreach.com
Sharon Trout	strout@troutreach.com
Jack Ungerleider	jack@jacku.com
Sharon Walbran	sharon.walbran@gmail.com

TC/PC Member Benefits

Product previews and demonstrations

Special Interest Groups
Monthly Newsletter

Discounts on products and services

Contests and prizes

Business Member Benefits

All of the above PLUS:

FREE ½ page ad on payment of each renewal

20% discount on all ads Placed in the *Digital Viking* Newsletter

Up to 5 newsletters mailed to your site (only a nominal cost for each additional 5 mailed)

Newsletter Staff

Editor Sharon Walbran

The following is from a letter received by Judy Taylour of APCUG from Malwarebytes.

The Conduent breach; from 10 million to 25 million (and counting)

by Pieter Arntz | February 26, 2026

The Conduent breach has quietly grown into one of the biggest third‑party data incidents in US history, and the real story now is how many different programs and employers are swept up in it, even for people who have never heard of Conduent.

-

When we first covered this incident, public filings suggested roughly 10.5 million affected individuals, heavily concentrated in Oregon and a few other states. Fresh state notifications reportedly put the total at more than 25 million people across the US, with Texas alone jumping from an early estimate of about 4 million to 15.4 million residents impacted, and Oregon holding at around 10.5 million.

-

That makes this one of the largest healthcare‑related breaches on record, with attackers reportedly spending about three months in Conduent's environment and exfiltrating around 8 TB of data.

-

How are so many people affected who have never heard of Conduent?

-

In 2019, Conduent said its systems supported services for more than 100 million people nationwide and served a majority of Fortune 100 companies plus more than 500 government entities. That shows just how broad the potential blast radius is, even if not all of those records were touched in this incident.

Conduent sits behind the scenes of a major portion of US public services and corporate back‑office work, which explains why the victim list looks so disconnected. Its platforms handle:

- State benefit programs such as Medicaid, SNAP (Supplemental Nutrition Assistance Program), and other government payment disbursements in more than 30 states.
- Mailroom, printing, and payment processing for state benefit offices and healthcare programs, including large health insurers like Blue Cross Blue Shield plans.
- Corporate services for major employers, including at least one large automotive manufacturer; nearly 17,000 Volvo Group employees are confirmed among those whose data was exposed.

Who stole what?
The cyberattack was later claimed by the SafePay ransomware gang.

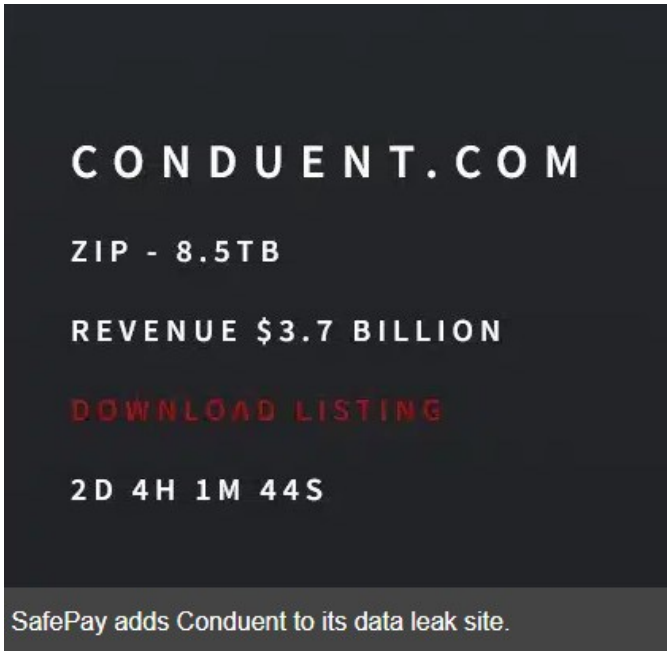


Image courtesy of Comparitech

The stolen data goes far beyond contact details. Notification letters and regulator filings describe:

- Full legal names, postal addresses, and dates of birth.
- Social Security numbers and other government identifiers.
- Medical information, health insurance details, and related claims data.

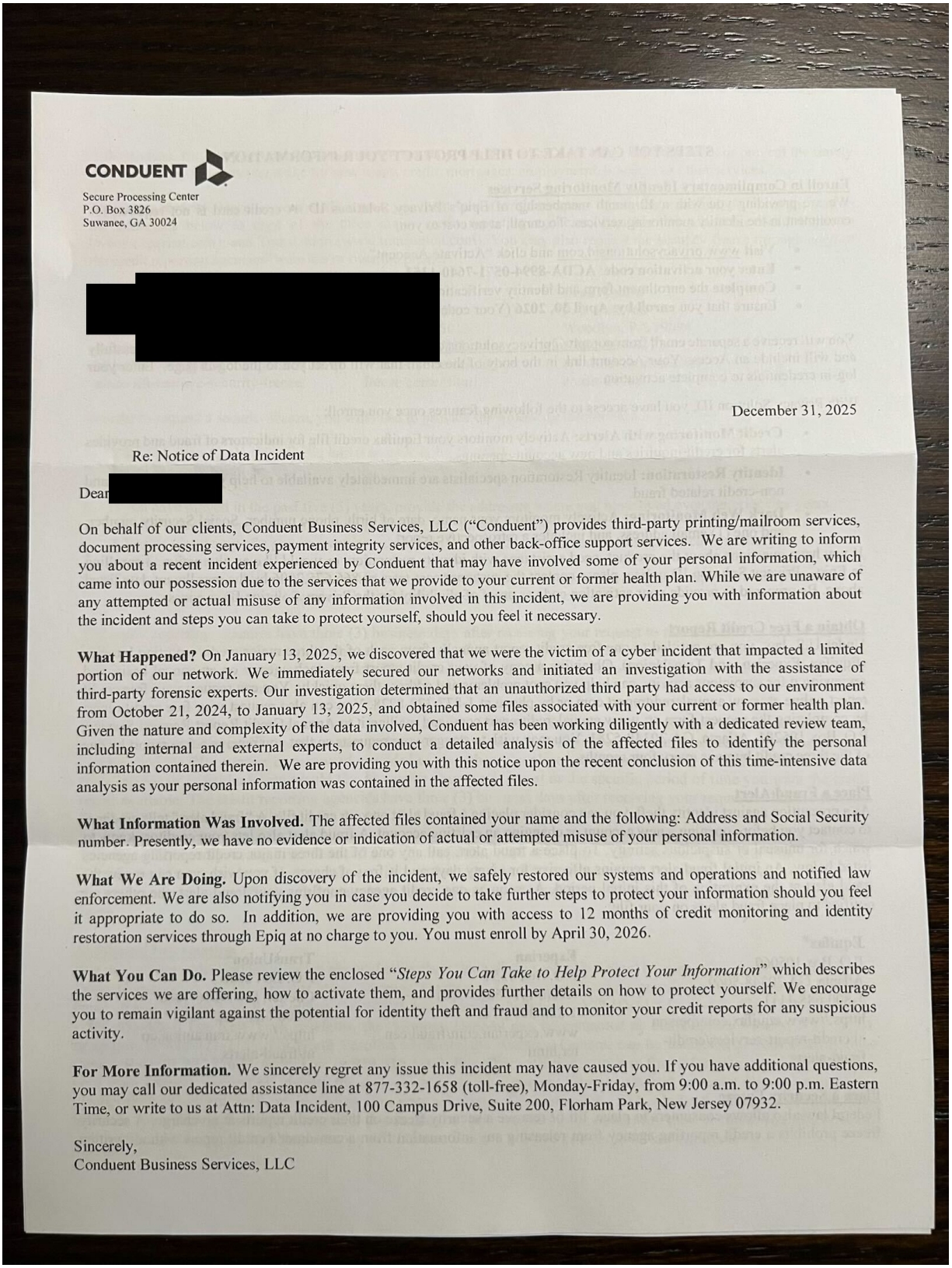
Because Conduent processes benefits and HR data on behalf of agencies and employers, most people affected never interacted with Conduent directly and may not even recognize the name on the envelope. If you received SNAP benefits, Medicaid coverage, other state-administered healthcare, or worked for an organization that outsources HR or claims administration to Conduent (or one of its clients), your data may have flowed through its systems even though your "customer relationship" was with a state agency, insurer, or employer.

Why this is worse than it first looked
There are three reasons why this follow-up story is more serious than the original:

- **More people are involved:** The raw numbers climbed from 10 million to 25 million as more states and corporate clients disclosed involvement, showing how opaque third-party breaches can be at the start.
- **Forever identifiers:** SSNs plus medical and insurance data enable long-tail identity theft, medical fraud, and highly targeted phishing that can haunt victims for years.
- **Third-party blind spot:** For many covered entities, "the breach" will never show up in their own logs because the compromise happened in a vendor's environment they rely on but do not control.

So when an unexpected letter from Conduent arrives, it's not a mistake. It's a reminder that your data can be put at risk far away from the organizations you thought you were dealing with—and that the real exposure from this breach extends well beyond the numbers in any single state filing.

[See Conduent letter on next page.]



CONDUENT

Secure Processing Center
P.O. Box 3826
Suwanee, GA 30024

[redacted]

December 31, 2025

Re: Notice of Data Incident

Dear [redacted]

On behalf of our clients, Conduent Business Services, LLC ("Conduent") provides third-party printing/mailroom services, document processing services, payment integrity services, and other back-office support services. We are writing to inform you about a recent incident experienced by Conduent that may have involved some of your personal information, which came into our possession due to the services that we provide to your current or former health plan. While we are unaware of any attempted or actual misuse of any information involved in this incident, we are providing you with information about the incident and steps you can take to protect yourself, should you feel it necessary.

What Happened? On January 13, 2025, we discovered that we were the victim of a cyber incident that impacted a limited portion of our network. We immediately secured our networks and initiated an investigation with the assistance of third-party forensic experts. Our investigation determined that an unauthorized third party had access to our environment from October 21, 2024, to January 13, 2025, and obtained some files associated with your current or former health plan. Given the nature and complexity of the data involved, Conduent has been working diligently with a dedicated review team, including internal and external experts, to conduct a detailed analysis of the affected files to identify the personal information contained therein. We are providing you with this notice upon the recent conclusion of this time-intensive data analysis as your personal information was contained in the affected files.

What Information Was Involved. The affected files contained your name and the following: Address and Social Security number. Presently, we have no evidence or indication of actual or attempted misuse of your personal information.

What We Are Doing. Upon discovery of the incident, we safely restored our systems and operations and notified law enforcement. We are also notifying you in case you decide to take further steps to protect your information should you feel it appropriate to do so. In addition, we are providing you with access to 12 months of credit monitoring and identity restoration services through Epiq at no charge to you. You must enroll by April 30, 2026.

What You Can Do. Please review the enclosed "*Steps You Can Take to Help Protect Your Information*" which describes the services we are offering, how to activate them, and provides further details on how to protect yourself. We encourage you to remain vigilant against the potential for identity theft and fraud and to monitor your credit reports for any suspicious activity.

For More Information. We sincerely regret any issue this incident may have caused you. If you have additional questions, you may call our dedicated assistance line at 877-332-1658 (toll-free), Monday-Friday, from 9:00 a.m. to 9:00 p.m. Eastern Time, or write to us at Attn: Data Incident, 100 Campus Drive, Suite 200, Florham Park, New Jersey 07932.

Sincerely,
Conduent Business Services, LLC

Conduent breach notification letter

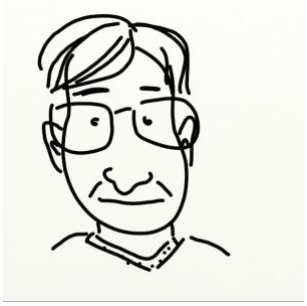
Depending on which of your data was compromised, you may receive a slightly different letter. If you receive one, you could read our guide on what to do after a data breach to understand your next steps.

We don’t just report on threats—we help safeguard your entire digital identity
Cybersecurity risks should never spread beyond a headline. Protect your, and your family’s, personal information by using identity protection.

SHARE THIS ARTICLE

Add as a preferred source on Google

About the author



Pieter Arntz

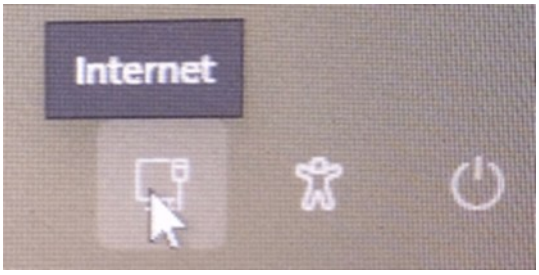
Malware Intelligence Researcher
Was a Microsoft MVP in consumer security for 12 years running. Can speak four languages. Smells of rich mahogany and leather-bound books.

Go to Page 1

“Help, Tom! I Forgot My Windows Login Password!”

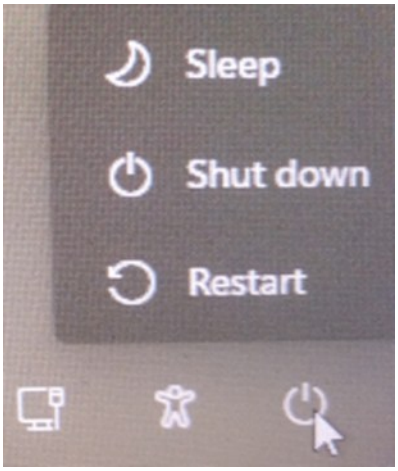
By Tom Burt, Vice-President, Sun City Summerlin Computer Club
https://www.scscc.club tomburt89134 (at) cox.net

Not long ago, a long-time friend emailed me in some desperation, asking for my help. She had been “cleaning up” her Windows laptop PC and at some point, she was no longer able to log in; her password, which had worked earlier in the day, was rejected as “incorrect”. I agreed to take a look and, if it looked beyond my skills, to advise her on what options she might have. This began a two week odyssey on my part to get the laptop back into a state where she could login and then to recover her data files, which we discovered had seemingly gone missing.



Let me call my friend “Amiga”, which is Spanish for “female friend”. (In Las Vegas, we all “hablamos un poco español”.) Amiga brought her laptop to Casa de Burt (my house), powered it up and showed me the login failure. She was pretty certain her Windows login was her Microsoft account.

We tried using her smart phone to log in to her Microsoft account and reset her password. We gave the laptop a couple of minutes to synchronize with the online Microsoft account and then tried logging in with the new password. (I determined later that this was useless because the laptop wasn’t connected to my in-house LAN.) Windows rejected the new password and also the old password.



At that point, I said I’d have to do some research on how to reset a forgotten Windows passsword. Amiga said, based on her own research before calling me, that if I clicked the power icon at the lower right corner of the Login screen and then clicked the Restart option while pressing the Shift key, it would boot into the System Recovery screens. Sure enough, it did. But she didn’t know what any of those screens did and was, wisely, uneasy about clicking around and intiating any actions.

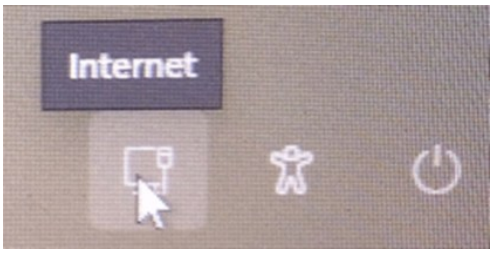
Note The icons only appear after you press Enter or click to display the password entry box.

We agreed I’d keep the laptop, do some research, and see if I could get in and reset her password.

Research

I set up Amiga’s laptop in my office, near my WiFi router and desktop to make it easier to do research and then try things on the laptop. It was fairly easy to use the Power > Shift+Restart sequence to get into the laptop’s Recovery environment and then go to: Advanced > Command Prompt. The Command Prompt would show it was running from the Recovery environment’s boot partition, labeled with drive letter X:. When I tried to switch to the laptop’s C: partition, I would get an error message saying I needed to enter a recovery key to access that partition. I didn’t have that recovery key. I didn’t initially appreciate the implications of that message.

Connecting the Laptop to the Internet



By then, it had also occurred to me that Amiga's laptop was set up to login using her Microsoft account credentials. But with the laptop at my house, it wasn't able to access the Internet because it wasn't connected to my in-house WiFi LAN. I noticed an icon at the lower right of the laptop's login screen that, when I hovered the mouse over it, displayed the word "Internet" I clicked the icon and got to a screen where I could connect the laptop to my in-house LAN's guest network. I gave it a few minutes to synch up with Microsoft's servers, hoping that the recently-changed Microsoft password would now work. But the laptop still rejected the password.

Consulting Gemini 3

I decided to consult Google's Gemini 3 AI on how to reset forgotten passwords. It offered up a very helpful discourse on the topic. In the Command Prompt, there's a command: NET USER that lets you list user accounts, reset the password of a specific user or to add a new user. Just what I needed! However, those commands apply to the current boot partition's registry. When running the Command Prompt from the Recovery environment, those actions were not affecting the users defined on the laptop's C: drive. So, time for more research.

BitLocker Surprise

I'd also come to the realization that, when initially set up by Dell, Amiga's laptop had Windows BitLocker encryption activated on the C: partition. This is now quite common. I spent another hour with Gemini, learning all the fundamentals of how BitLocker worked and how to locate the **48-digit BitLocker recovery key** for Amiga's laptop on her Microsoft Account. It's kept at:

https://account.microsoft.com/devices/recoverykey .

Once I had that recovery key, I could manually enter it in the Recovery environment's Command Prompt and finally have access to her laptop's C: drive. My first action was to plug in a flash drive and copy all her data files from the C: drive to the flash drive.

It had gotten late, and I decided to shut down Amiga's laptop for the night, planning to pick up the troubleshooting the next morning. However, the attempt to shut down reported that Windows Updates were in progress and to not power off. I finally left the laptop running overnight. The next morning, I found the laptop shut down. I powered it up and got to the login screen. I hopefully tried various passwords, but all were rejected.

Consulting Gemini 3 Again

I consulted Gemini 3 again, this time asking how to reset a password when the C: drive was encrypted with BitLocker. Gemini returned another sympathetic, but helpful exposition outlining the steps needed to get to a Command Prompt operating on the unencrypted C: drive.

The key step is to take advantage of an icon on the login screen that launches the Accessibility Settings applet (utilman.exe). Once connected with the Recovery environment's Command Prompt to the unencrypted C: drive (by entering the 48-digit recovery key), here are the commands to type in:

1. CD C:\Windows\System32 *Navigates to the correct folder*
2. copy utilman.exe utilmanback.exe /Y *Backs up utilman.exe*
3. copy cmd.exe utilman.exe /Y *Copies cmd.exe over utilman.exe*
4. Exit the command prompt
5. Exit the recovery environment, choosing to boot normally.

Resetting the Forgotten Password

The login screen will appear. Press Enter to show the "Accessibility" and "Power" icons at the lower right. Click the "Accessibility" icon and it will launch utilman.exe, which is actually now a copy of cmd.exe. Shazaam! A Command Prompt window opens from the now-accessible C: drive. Once in this state, it's possible to use the NET USER and NET LOCALGROUP commands to reset the forgotten passwords and to create a separate local administrator account.

Here are the commands I typed to reset Amiga's password on the laptop:
1. NET USER *Lists the current user accounts (to be sure of spelling)*
2. NET USER amiga * *Initiates a reset of the password for Amiga's account*
3. Enter the new password *I used her latest Microsoft account password*

Confirm the new password

Creating a New Local Administrator Account

Here are the commands to add a new local administrator account: "amigaadmin".
1. NET USER amigaadmin * /Add *Creates the new user*
2. Enter the password for amigaadmin *Her latest Microsoft account password*
3. Confirm the password
4. NET LOCALGROUP administrators *Lists the current administrator accounts*
5. NET LOCALGROUP administrators amigaadmin /Add
   This Makes amigaadmin an administrator.

I decided to add the local administrator account so that if future problems developed with Amiga's regular Microsoft account, there would be an alternative way to login to the laptop and do system mangement without needing to resort to these back door methods.

I tested both logins and they both worked. I was able to get to the Windows desktop and all the regular windowed interfaces worked. A final step was to restore utilman.exe so that the icon on the login screen actually launches the Accessibility settings. This required once more clicking the Power icon on the login screen, Shift-clicking the Restart option to reach the Recovery environment, selecting Advanced and the Command Prompt and then entering the 48-digit BitLocker recovery key to access the C: drive. Here are the commands to restore utilman.exe:
1. CD C:\Windows\System32 *Navigates to the correct folder*
2. Copy utilmanback.exe utilman.exe /Y
3. Exit the command prompt

Reboot normally

On the login screen, clicking the Accessibility icon will again display the Accessibility settings screens.

Where Did the Data Go?

Once I got logged in to the laptop (as Amiga), I did some checking in Windows Update and found

that Windows 11 had updated itself to version 25H2. Everything seemed to work, but I was suspicious because there were no third-party apps installed and a lot of the data file icons in the OneDrive folder didn't launch any app when clicked. The laptop was also very sluggish. Clicking on things would take several seconds before there was any visible response on screen. This laptop had only a 5400 RPM hard drive – no solid-state drive.

I had Amiga come back to my house to check things out. She said that many items from her desktop were missing. It appears that in her own attempts to resolve the login problem before calling me, she may have initiated a factory reset. The Windows event logs were inconclusive. It did look like most of her data files were backed up to her OneDrive cloud storage on Microsoft. But the laptop didn't seem to be connected to that cloud storage, even though it was logged in using her Microsoft Account. Amiga took the laptop home. She planned to access her OneDrive cloud storage from her other Windows PC, download the data to a flash drive and then load it from there onto the laptop. I got an email from her that night saying when she tried to login to her Microsoft account, she got rejected with an "invalid password" error.

Since I had the credentials for Amiga's Microsoft account, I tried logging into that account using my web browser and got in with no problems. I then browsed to her OneDrive cloud storage and confirmed all the missing data files were there. I downloaded a copy of everything to my own desktop's hard drive. I sent Amiga a note with directions on what I'd done to download the data. And that's where things stand. She's been busy with other things and set the laptop aside.

Conclusions

There are several morals to this story:

A key one that can't be stressed enough is that you MUST back up your data files – not just to the cloud, but also to local storage media, like a large flash drive or external USB drive. This has to be done regularly – once a week, once a month. Backups that are months out of date don't help much when you need to recover your current operational state.

Set up an emergency local administrator account with a known password. You only login to this account if something goes wrong with your primary login. Have those credentials written down and saved in a paper folder or envelope.

With laptops or desktops that come with BitLocker encryption enabled on the system drive, consider spending the time to turn BitLocker off. It will take some time for Windows to unencrypt the data, but it will make recovering from a forgotten or inadvertently changed password much easier. That setting is in Control Panel > BitLocker Drive Encryption.

If you DO want to keep BitLocker encryption, be sure to retrieve your drive's 48-digit BitLocker Recovery key and print it out on paper. File this in the folder/envelope with the credentials for your emergency adminstrator account.

If you're buying a new Windows 11 desktop or laptop, be sure to get a model that has a solid-state drive of at least 256 GB capacity for the system drive; 512 GB is better. Windows 11 is just too resource-hungry to be usable on a 5400 RPM laptop hard disk drive.

Lastly, be mindful that Microsoft has engineered Windows 11 to be very difficult for ordinary consumers to troubleshoot. Sometimes it's better to get skilled help from the start, rather than poke around on your own. In our club, the Repair SIG team has a lot of experience dealing with the issues I've described above. We also have several capable members willing to make a house call (for a modest fee) to help you..

Meetings start at 7:00 PM (9:00 AM on Saturday) unless otherwise noted. *Virtual Meetings during Covid pandemic..

March

April

SUN	MON	TUES	WED	THU	FRI	SAT
1	2	3	4	5	6	7
8	9	10 7pm General Mtg Best of the CES 6pm Tech Topics	11	12	13	14 Canceled Linux on Saturday SIG 9:00-Noon
15	16	17	18	19	20	21 MS Office SIG (includes Access) 9:00-Noon
22	23	24	25	26	27	28
29	30	31	1	2	3	4
5	6	7	8	9	10	11 Canceled Linux on Saturday SIG 9:00-Noon
12	13	14 7pm General Mtg TBA 6pm Tech Topics	15	16	17	18 MS Office SIG (includes Access) 9:00-Noon
19	20	21	22	23	24	25
26	27	28	29	30		

Go to Page 1

Twin Cities PC USER GROUP

You have just read an issue of The Digital Viking.

Would you like to receive this delivered directly to your email or business each month?

As a member of TC/PC, the Twin Cities Personal Computer Group, one of the benefits is reading this monthly publication at www.tcpc.com..

As a member of TC/PC, you may attend any or all of the monthly Special Interest Group (SIG) meetings and be eligible for software drawings. The small membership fee also includes access to real-live people with answers via our helplines, discounts, and various other perks.

Does membership in this group sound like a good way to increase your computer knowledge?

It's easy to do! Simply fill in the form below and mail it to the address shown.
(If you use the form in this issue, you will receive an extra month for joining now.)

3/26

Here's the info for my TC/PC Membership:

Full name_____

Company name_____

Address_____

City_____ State_____ Zip_____

❍Home ❍Business ❍Change address: ❍Perm. ❍Temp. 'til _____

Home phone_____ Work phone_____

Online address(es) _____

Where did you hear about TC/PC? _____

❍ I DO NOT want any of my information disclosed.
❍ I DO NOT want to receive any mailings

Administrative Use Only Rec'd_____ Chk#_____

I'm signing up for3

❍ Individual/Family Membership ($9)
❍ Business Membership ($100)
If an existing member your # _____

Make checks payable to:
Twin Cities PC User Group
341 County Rd C2 W
Roseville, MN 55113

Or sign up on our website:

http://www.tcpc.com

❍ Check #_____ ❍ Bill me
❍ New member ❍ Renewal ❍ Prior member

I'm interested in:
❍ Training classes ❍ Volunteering
❍ Special Interest Groups: New User, Access, etc.
List here:

March 10, 2026

7:00 pm

General Meeting

Best of the CES 2026!

Via Zoom Only

Twin Cities PC USER GROUP

341 County Rd C2 W
Roseville, MN 55113

FIRST CLASS MAIL