IT Department

May 2024

NewsLetter

Headlines: Why Battery Backups \ Don't Take The Bait \ Passwords \ The Story, Part 1 \ Oh My Eye Funny Pages, May theme is "Summer" \ "New" Notice of the Month

---

Why Battery Backups (UPS) Are Essential for Saratoga Bridges

Power outages and surges can wreck your equipment and cost Saratoga Bridges thousands in lost productivity and lost equipment costs. That's why we invest in battery backups, or Uninterruptible Power Supplies (UPS)—especially for computers, towers, and network gear.

What Does a UPS Do?

A UPS keeps your equipment running when the power goes out, even if just for a few minutes. That time allows you to save your work and safely shut down—preventing data loss, hardware damage, and costly downtime.

Save Your Computer, your work—and our Budget

Replacing one damaged computer can cost $1000 or more.

Average downtime for a small business can cost $10K–$25K per hour--for us services are mission critical. We can't afford to not be able to deliver services.

A good UPS costs around $100–$300—and can extend your computer and monitor's life by up to 30%.

Best Practices

Plug in to UPS: **desktops, network equipment, game systems, routers, modems.**

Don't Plug in: **Don't plug laser printers and copiers into battery backups—they draw too much power and shorten UPS life.**

Choose the right UPS: **make sure the wattage matches what you are drawing--call tech support to find out if you need a larger UPS.**

Plug your location's internet router into a UPS, **this will keep the internet up when the power goes down.**

Common Mistakes

- **Don't ignore UPS alarms or dead batteries.**
- **Don't plug power strips into UPS outlets.**
- **Don't use a UPS that is too small for your usage -- contact tech support if you aren't sure!**

Final Word

Think of a UPS as electrical fire insurance, and work insurance—it's an affordable way to protect our equipment, your work (data), and maintain Saratoga Bridges services even if the power is out.

Please Read and Don't take the Bait: How to spot a Phishing Email

Before I begin this long journey of what's been said to be one of the most simple but yet most dangerous or harmful methods of steeling ones identity or financials, I will bore you with the all too common question " Why am I receiving this email?" If you have to ask yourself this question, there is a good chance that you don't need it and you can delete it.

In the past month, there seems to be an uptick in Phishing emails. Not just here but across all continents. Some are blamed on world news or possible political gain and others are blamed on the economy. The primary purpose of Phishing email attacks are, bad actors looking to take your valuable information or personally identifiable information or PII, log in credentials for bank accounts, credit card, and so on.

How do they get this information? They lure ("Phish") you in by sending you legitimate looking emails that seem to be innocent advertisements that send you to dangerous websites. Even worse, emails from attackers posing as family, friends or work colleagues that have links or attachments that prompt you to enter your credentials in order to open them. The latter of the two seem to be have a greater chance of impacting you because they have already gained your trust by posing as your loved ones or work colleagues and have provided you with an attachment that was meant for you and not just the general public.

What to do if you do receive an email with an attachment from someone that you are NOT expecting anything from:

Please delete the email and then **CALL the sender directly.**

Do NOT reply to the email asking them if they sent you this email and "is it safe to open". They may actually reply to you and say "Yes, I did send you the email and it is safe to open and or click on the attachment" **DO NOT DO THIS!** With A.I , the reply may not even be human. Did you know that once you have fallen victim to a Phishing email and your account/s has become compromised, that even if you create a new email and send it to the bad actor, A.I. will reply back to you stating that it is ok to open the email that was just sent to you. This is why it is best practice to call the person directly. I believe this too will have its faults in the future, **but until then, CALL!**

How to Manage Your Passwords (Without Losing Your Mind)

Passwords are unavoidable. Every site and app require one, but weak password habits can leave you vulnerable to hackers. Managing them properly is not just smart — it's necessary.

Why Browser Password Managers Aren't Safe

Browsers like Chrome, Safari, and Firefox offer to save your passwords. It's tempting, but risky. Browsers aren't built for serious security. If someone gets into your computer, they can often view your saved passwords easily. Malware specifically targets browser-stored passwords, and if your Google or Apple account is compromised, everything saved in your browser could be exposed.
In short: *your browser's built-in memory isn't secure enough*.

Smarter Ways to Manage Passwords

Instead of relying on your browser, use a better system:

- Password Managers: Apps like 1Password, Bitwarden, and Dashlane encrypt your passwords, generate strong ones, and autofill them securely across devices.
    - Bitwarden: Offers a great free plan — unlimited passwords, syncing across devices, password sharing, and secure notes. It's open-source and regularly audited.

    - 1Password: Paid-only, but offers a slicker interface, family plans, dark web monitoring, and top-notch customer support.
    - Dashlane: Free plan includes 25 passwords on one device. Premium plans add unlimited syncing, VPN services, and dark web alerts.
- Physical Security Keys: (significant initial cost)
    - A physical security key is a small device (like a USB stick) that acts as a "lock" for your online accounts. Even if someone steals your password, they can't log in without the physical key. Brands like YubiKey and Google Titan Security Key offer reliable options.
    - Security keys use protocols like FIDO2 and U2F to authenticate your identity without needing a password alone. They're excellent for protecting important accounts — email, banking, cloud storage — and are becoming the gold standard for two-factor authentication (2FA). They're simple to use you plug it into your device (or tap it via NFC on your phone) when logging into supported services.
- Encrypted Offline Storage: Some prefer storing passwords in a strongly encrypted file, but it's less flexible and riskier if you lose access.

How to Create Strong Passwords

Strong passwords share three traits:

- Long: At least 16 characters — longer is better.
- Complex: Mix uppercase, lowercase, numbers, and symbols.
- Random: No real words, no personal info.

Bad example: ***Summer2024!***
Good example: ***9fT$kz!wQ0GmP8vhz@2I***
Don't try to memorize hundreds of passwords. Let the password manager handle it.

Good Password Habits

Strong passwords alone aren't enough. Build smarter habits:

- Use a unique password for every account.
- Turn on two-factor authentication (2FA) — using an app or a security key.
- Change important passwords regularly.
- Always verify password reset emails.

Quick Takeaway

- Don't trust browsers to save your passwords.
- Use a dedicated password manager like Bitwarden, 1Password, or Dashlane.
- Consider adding a physical security key for critical accounts.
- Make passwords long, random, and complex.
- Turn on 2FA wherever possible.
- Stay alert to phishing and scams.

A little work now beats dealing with a hacked account later. If you wish to set up a password manager like any of the above-mentioned and require assistance, please contact the IT dept, we are happy to help.

The story behind the Designated Records Set

Part 1

Yes. Stories are told to serve a purpose and what gets looked at is often closely related to this purpose. There is a story behind the Designated Records Set and we'll focus on the one that is most effective when we need to decide which version to use. But, first, what is this Designated Records Set, or DRS as we call it? We'll get to know when to use the versions later.

Saratoga Bridges uses a fee for service business model where we get compensated for the documented work of the staff. Therap is where our work gets documented. When you take attendance, file a GER, submit billing, and so on, Therap must be set up to make these tasks possible. The set up is the group of records or data points designated as being required for those tasks mentioned here and many others. With this background, let's turn our attention to the purposes the DRS serves. This will shed light on why we have three versions and when to use them.

It helps to think about the time individuals spend in our programs has having a beginning, a middle, and an end. It's a story. The *DRS-Admission* is the beginning. The *DRS-Transfer/Change* is the middle. The *DRS-Discharge* is at the end. Each of these serves its unique purpose and is used to move the individual into and out of our programs. Finally, when do we use each version? We'll cover these points in the second part of this story.

Eye Strain for Computer users:

To minimize eye strain when using a computer, make adjustments to your workstation, take frequent breaks, and ensure good lighting. Additionally, consider using eye drops and adjusting your monitor settings for optimal viewing.

Adjusting your workstation:

- Monitor Position:

Place your monitor about an arm's length away, with the top of the screen slightly below eye level.

- Lighting:

- Ensure the screen's brightness matches your surrounding workspace. Consider using ambient lighting to avoid glare and reduce the contrast between the screen and your environment.
- Work Surface:

Place reference materials above the keyboard and below the monitor to minimize the need to move your head and neck, according to the American Optometric Association (AOA).

Taking breaks:

- **20-20-20 Rule:** Every 20 minutes, look at something 20 feet away for 20 seconds.
- **Blink Frequently:** Be mindful of blinking more frequently, especially when working at a computer, as blinking helps keep eyes moist.
- **Short Breaks:** Take 10-minute breaks every hour to rest your eyes.

Adjusting your screen settings:

- **Contrast and Brightness:**

Adjust your monitor's contrast and brightness to a comfortable level.

- **Font Size:**

Increase the font size to make text easier to read, suggests Harvard Health.

- **Color Temperature:**

Consider changing the color temperature to reduce blue light, especially if you're working late into the evening.

- **Blue Light Filters:**

Asurion suggests avoiding blue light filters, as they can actually reduce the clarity of the screen.

Other helpful tips:

- **Eye Drops:**

Use **artificial tears** or lubricating eye drops to relieve dryness and irritation

Computer Glasses:

Consider using specialized computer glasses or reflective lenses, as they can reduce glare and blue light, says Charlotte Optometry.

Notice Of The Month

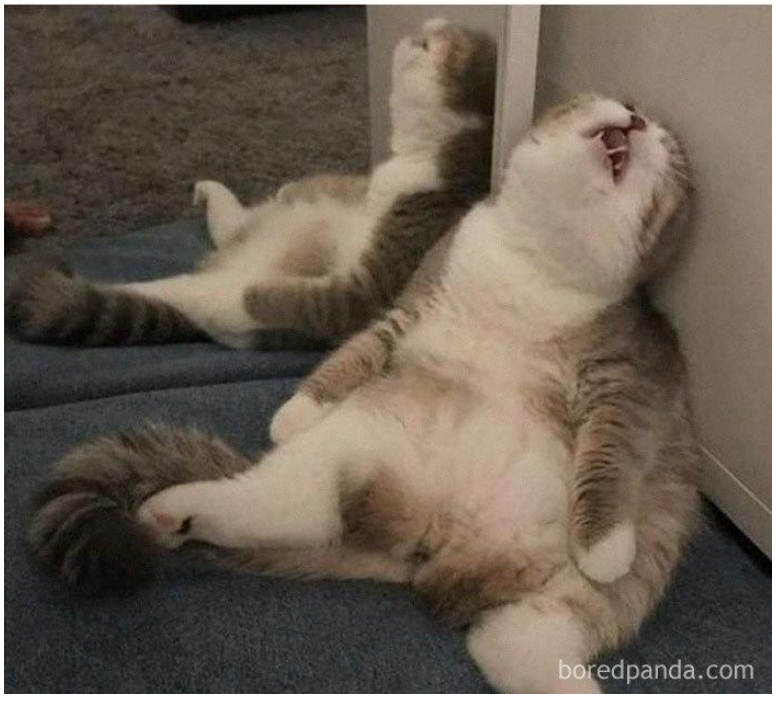
Please Sign Out Of Your Zoom

The Funny Page

Theme

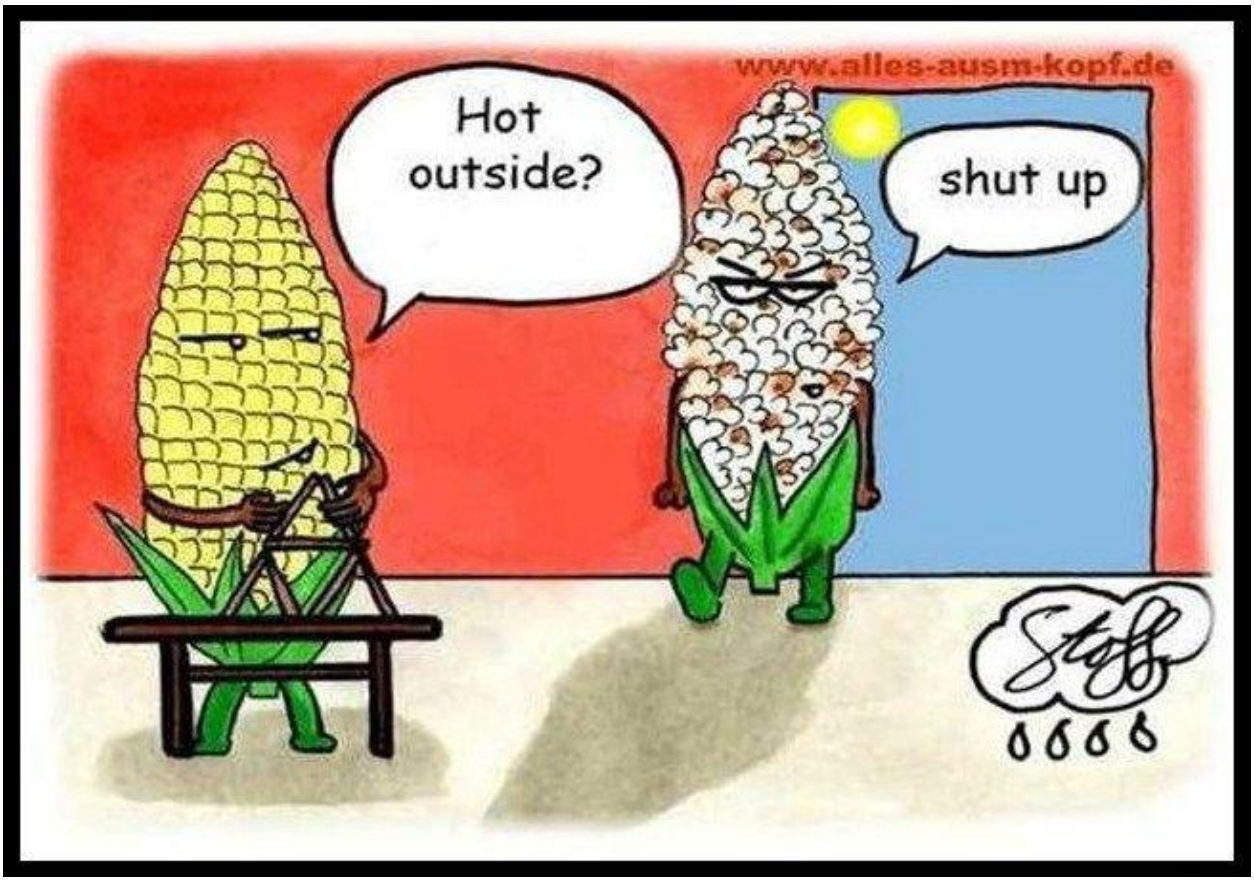
“ Spring time ”

When you need to clean but have no motivation so you just sit there for a while like



" We've got to do spring cleaning more often.
I found three *eight-track tapes!* "

At least the mess I make is
all in one place



When The Stickler Speaks, More About AI, **PC Game Systems**, New Computer Desktop & Sign On, **coming soon** **"Spotlight" and much much more..**

Send comments to: Editor - Phil Ellsworth

pellsworth@saratogabridges.org

More Content coming soon....