



Back to School Cybersecurity Tips

Be Alert for Cyber Scams

The new school year is an exciting time for students, faculty, and staff. It's also an exciting time for hackers, identity thieves, and other unscrupulous types who take advantage of people during this busy time of year.

Watch Out for Typical Beginning of the Year Scams

- Emails supposedly containing "important information about your school account," or a "problem with your registration"
- Scams specifically designed to cheat students out of money, such as scholarship scams, fake "tuition payment processors", textbook rental or book-buying scams, housing scams, tutoring scams, and work-from-home scams
- "Tech support" scams where you get a call supposedly from "the Service Desk" or even "Microsoft" or "Apple" telling you there's a problem with your computer
- IRS impersonators demanding that students or their parents wire money immediately to pay a fake "federal student tax"



- Messages asking for your login information, no matter how legitimate they may look. No one other than you need to know your passwords
- Fake friend requests on social media
Fake Box or Google Doc notices

How to Stay Safe

The best way to avoid scams is to have a healthy skepticism.

1. Always think twice before clicking on links or opening attachments, even if they look like they're from someone you know. If you're not sure, contact the sender by a method you know is legitimate to confirm they sent it.
2. Verify requests for private information. Remember, con artists know how to fake their identity.
3. Protect your passwords. Make them long and strong, never reveal them to anyone, and use different passwords for different accounts.

What Happened to My Data?

The Dangers of Insufficient Backup Procedures

With today's businesses operating at breakneck speed, the strain placed on IT networks has exposed small to mid-size businesses (SMBs) to more security threats than ever before. Factor in the persistent threat of natural disasters, power outages, human errors and failed system upgrades, and the dangers of having an insufficient data backup procedures become abundantly clear.



Failure is not an option

Failing to address these risks can cause severe network damage and immobilize a company for hours, days or even weeks. The best way to combat this dynamic is to understand the risks, address the problem, and make sure the proper precautions have been taken.

Partial data loss can still be devastating

Despite the countless ways data can be lost, many businesses lack a comprehensive data backup procedure. According to Symantec's 2011 SMB Disaster Preparedness Survey, "only half [of SMBs] back up at least 60% of their data, meaning they would lose 40% of their data in the event of a disaster." What's more, 31% of businesses surveyed don't back up email, 21% don't back up application data and 17% don't back up customer data.

If your data gets lost, the best-case scenario is that your employees have to re-do some work; the worst-case scenario is that the data is gone forever. By maintaining a data backup solution, you can ensure that all of your

important files can be recovered quickly, fully and with minimal effort.

It's not just your organization that is impacted

As stated earlier there is a major impact that data loss has on your own business. In addition, the lack of a back-up plan could affect relationships with your customers. Businesses that are subject to compliance or regulatory standards must ensure that all company endpoints are protected in an appropriate fashion. This is why having an automated or regularly scheduled backup procedure is immense. According to Enterprise Security Group, even with all the advancements in storage technology, only about 20% of backup jobs are successful. This makes consistency and frequency key metrics in evaluating any backup solution.

A cloud backup solution is ideal

It's important to be mindful of how you're backing up your data. For example, leveraging outdated equipment such as tapes, disks and other types of hardware is risky because these solutions can be lost, stolen or improperly stored. Any of these outcomes usually results in the data becoming irretrievable. Modern disaster recovery solutions address these risks and provide a software-based solution that virtualizes all data to the cloud. This enhances overall performance by providing greater accuracy, efficiency, security and archiving functionality to a business's disaster recovery plan.

Simply put, technology has come too far for SMBs to have to deal with the risk of data loss crippling their business. With today's powerful solutions and the availability of trusted IT advisors like BrevAll Technologies, SMBs can protect themselves, their employees and their customers' data from these threats.

If you're in need of a comprehensive modern backup strategy, then contact the backup solution experts at BrevAll. We'll assess your needs and develop a comprehensive plan customized to fully protect your organization from the devastation from data loss.

Protecting Your Network Assets with Multi-Factor Authentication (MFA)

Passwords are no longer sufficient to secure logins, with 81% of breaches involving weak or stolen passwords. Multi-factor authentication (MFA) protects users from attacks by ensuring that only the intended, authorized users can access critical, secure information.

The access to fast Internet allows employees to work from anywhere – their homes, hotels, coffee shops. Corporate information is no longer concentrated in server rooms or data centers on premises; it is distributed in the Cloud.

Every day an employee will certainly authenticate to several online services. First, to their computer. If they are not physically in the office, they are probably connecting to the network through a VPN where the data traffic carries user credentials through Wi-Fi connections and public networks.

If at some point those credentials are exposed, what are the odds that the same password is used on most of the other services? The chances are high. With dozens of credentials to remember every day who would intentionally select a different password for each of the services they access?

A password that is captured when accessing your favorite website is likely to be the same password used to log in to your computer, or even the company VPN. Also, you don't know if an employee has used the same password for a personal service, or if they shared the password with someone.

All of that is to say that we can't trust passwords. They can be shared, written down, captured, guessed, cracked, and stolen.

Multi-Factor Authentication

Historically, the term "two-factor authentication" or "strong authentication" refers to when you use two of the following factors in order to authenticate to a network or digital service:

- Something you know: a password, a PIN
- Something you have: a token, a physical device, a key
- Something you are: your fingerprint, face recognition

The technology evolution, especially with smartphone usage and app development growth, opened the possibility of putting together more factors, without compromising usability. When two or more factors are used, we now call it multi-factor authentication (MFA).

The use of MFA enhances the overall security of the solution, offering additional protection against several types of attacks such as social engineering and RATs (Remote Access Trojans) designed to clone applications.



BrevAll congratulates two of our team members on achieving their Microsoft MS900 Fundamentals certification.



Mike Smith



Jason Perry

Microsoft 365 Certified
Fundamentals



N. Smith
John Smith
Chief Executive Officer



THE WOMEN'S CENTER

Who They Serve

Every day, women, men, and children in our community face sexual abuse, violence, poverty, and mental health issues. Many are struggling to find a way forward.

The Women's Center programs exist to empower them to do so, and build better futures for themselves and their families.

Their Programs Offer Hope

For more than 40 years, The Women's Center has inspired and empowered women, men, and children in the Tarrant County community to overcome violence, crisis, and poverty. Through four comprehensive programs, they help people triumph in the face of overwhelming obstacles and discover a path to a brighter future. In 2019 alone, their programs served 155,396 women, men, and children.

- Rape Crisis & Victim Services
- Violence Prevention & Education
- Employment Solutions
- General Counseling

How You Can Help

Everyone has a part to play, so we encourage you to get involved and give hope to those in need. To make their work possible, The Women's Center relies on the generosity of our community. They make it a priority to be good stewards of all that they receive and to be transparent in all they do.

<https://www.womenscentertc.org/donate-online>



BrevAll has been a proud partner of The Women's Center for over 15 years. We were honored this year as being the team with the third largest participation in this year's Victory Over Violence event.

BrevAll Technologies Monitors the Dark Web to Keep Customers' Information Safe

Stories of mass data breaches perpetrated by cybercriminals have become commonplace in the mainstream media. These breaches, which often affect hundreds of millions of individuals, invariably lead to identity theft, corporate intrusion, and other forms of cyber abuse. BrevAll has taken a proactive step not only to address this rampant source of criminal activity but also to put an end to its effect on small to medium-sized businesses (SMBs).

What Is the Dark Web?

While the Dark Web — the part of the internet that is not indexed by search engines and, therefore, not “Google-able” — is not a household term, it’s poised to become one. The Dark Web forms a small part of the deep web, a shadowy realm that attracts those who wish to act in secrecy, often to engage in illegal activity. The Dark Web is a place where individuals go to purchase illegal drugs, hire illicit acts, or hire hackers to attack specific businesses. It’s also a place where email addresses and passwords are available for purchase.

Most business owners who are only casually familiar with the Dark Web think the best thing they can do is to stay away from it and ensure their employees aren’t involved. This stance diminishes the threat of the Dark Web and puts your business at risk.



Unfortunately, most businesses are grossly under informed about the Dark Web and how it can affect them,” said Enloe. “Business owners need to know that company logins, passwords, identities, hackers for hire and bank accounts are all for sale on the Dark Web and that no governing body regulates this part of the internet. It’s the new Wild West.”

How BrevAll Can Help Protect Your Organization

BrevAll can scan the Dark Web and immediately determine if client emails and passwords are available for sale, making it an excellent solution for businesses concerned with the strength of their network security in this increasingly dangerous digital world.

The Dark Web is an unfortunate reality that business owners need to be aware of, but if there’s a bright side, it’s that it’s ushering in higher standards for data security, privacy, and cyber-protection. Once addressed, SMBs can get back to business as usual without wondering if their business is unnecessarily exposed to cybercriminals.

BrevAll leverages sophisticated Dark Web intelligence technology to identify, analyze, and check for compromised customer and employee data,” said Paul Enloe, CEO of BrevAll. “Cybercrime is rapidly on the rise in the United States, and SMBs need to know if their information is on the Dark Web.

COMING SOON

OUR NEW & IMPROVED WEBSITE

BrevAll will soon be launching our new website. In addition to having a fresh new look, the site will serve as a portal for learning about new and important technologies, while also providing helpful customer support options.

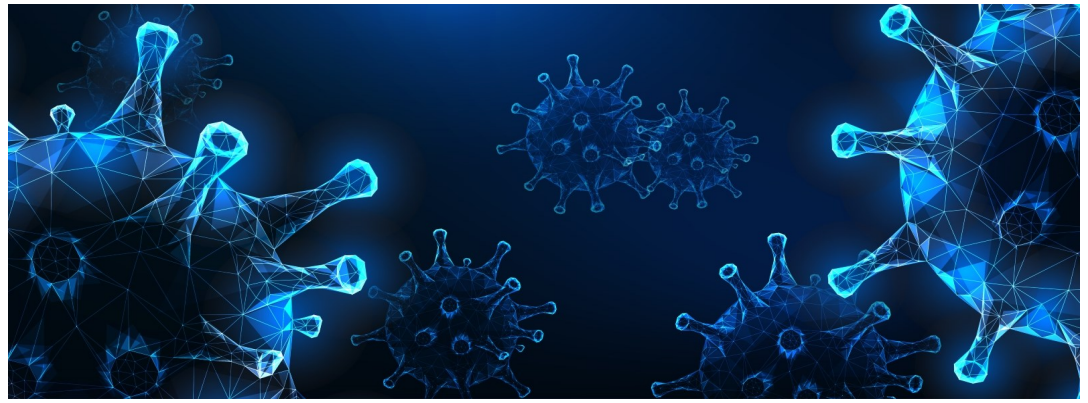
Here are some of the new features to look forward to seeing at www.brevall.com:

- Live Chat Support
- New Technology & Service Offerings
- Community Involvement Spotlight
- Video Customer Testimonials

We are excited about going live soon with the new website, and look forward to providing our customers with this new more informative and more interactive experience.



BrevAll Helps Businesses Persevere through the Pandemic



BrevAll specializes in building technology plans for businesses to continue to operate through the pandemic. We begin by evaluating an organization's existing technology and then create a plan to maximize operations and employee productivity with the proper technology that supports both remote and on-site workers. While more restrictions may be on the horizon, there is no reason why most businesses cannot adapt and thrive, especially when they have a strong technology plan.

We are in unprecedented times, but this doesn't mean businesses can't continue to flourish. With a shift in approach and proper technology, a business can set itself up for successful continued operations. Our technology plan is a simplified solution and consists of five main components.



1. Ensure Effective Voice Communication

Not all business phone systems are created equal. Many small to mid-sized businesses that use older systems faced severe challenges sending their employees home with the expectation to communicate effectively with customers and fellow employees. On the other hand, those companies that leverage today's cloud voice technology experienced a much easier and seamless transition.

2. Cybersecure the Home Office

With 45% of home office PCs being infected with malware, most companies' critical information is at risk. Protecting home office PCs must be done with the same due diligence as PCs in the office. Cyberattacks are at an all-time high and hackers are preying on remote workers with greater frequency since the pandemic started.

Continued on page 8

A New Kind of Community

Owenwood's dream is to create a community where their neighbors are known, heard and invited to use their gifts to transform Far East Dallas. Owenwood collaborating with many local organizations so their neighborhood can flourish. This is done through creative partnerships with existing nonprofits, bold initiatives born out of the dreams and talents of their neighbors, and the willingness to take risks on behalf of the Gospel.

Their mission is to create a space where the Spirit of God is followed, not doubted. Their commitment is the formation of a new faith community grounded in justice, equality, and opportunity for all who live in Far East Dallas.



REV. JOSH ESPARZA
CAMPUS PASTOR

Owenwood Leadership

Josh was appointed to Owenwood Farm and Neighbor Space in 2018. Josh is an advocate for asset-based community development and believes churches should play a vital role in that process. You'll find Josh talking with people from the neighborhood, planning worship, and meeting with people who are looking for a way to experience their faith differently. Josh considers himself a foodie and coffee connoisseur, so he and his wife, Victoria love to explore Dallas to find the best food/coffee spots.

How BrevAll Delivered on Owenwood's Needs

We consulted with the organization's leadership, and developed a customized comprehensive solution that met each of their needs while also staying within their budget. Our scope of work included the following:

- Complete Cabling Infrastructure upgrade
- Enterprise grade Firewall implementation for Cyber-Security
- Wifi Access Points
- Enclosure Wall Mount Rack with switches and patch panels

"BrevAll made redoing the internet infrastructure as seamless as possible. Excellent customer service, and always willing to work within our needs and price range."

– Rev. Josh Esparza, Campus Pastor



Continued from page 6

3. Proper Remote Workforce Management

BrevAll Technologies is a premier Member of Technology Assurance Group, an organization of leading managed technology services providers (MTSPs) in the United States and Canada, representing \$500 million in products and services. As a result, BrevAll Technologies possesses the proper techniques and processes to successfully manage a remote workforce. In return, BrevAll Technologies teaches its customers these best practices so they can be successful in maximizing the performance of remote employees.

4. Ensure the Home Office is Functional

One of the best practices for managing a remote team is to meet over video conferencing as frequently as possible, instead of just via phone call. Employers need to make sure that employees have a functional home office with a PC/laptop that has a camera and mic to get the most out of videoconferencing meetings. Some employees also need access to a Printer/Scanner, in case the office is not fully paperless, yet.

5. Provide Necessary Collaboration Tools

Without being in physical proximity, employees must rely on collaborative tools like Microsoft Teams, video conferencing and instant messaging more than ever before, so these solutions need to be carefully selected so that they integrate well. Microsoft Teams comes with all of those features already built-in but employees need to know how to get the most out of it.

Let BrevAll Guide You through the Tech Turmoil

BrevAll Technologies custom-tailors technology plans to meet specific needs for continued operations. We're taking a leadership position in the face of our current collective predicament, and proactively helping our customers persevere through restrictions or reopening guidelines.



Leveraging technology to improve and protect your business.

Brevall Technologies works with the industry leaders in cybersecurity and dark web monitoring to ensure our customers and their vital information are always secure.

817.589.0808 | www.brevall.com | info@brevall.com