The Tech chronicle

August 2022

This monthly publication is published for family, customers and friends of

BRANDON BUSINESS machines

Our business is taking care of your business.

Creating a Safe Online Presence For Your Children

In 4 Easy Steps

Children in this day and age are growing up in a technological climate that many of us never could have imagined 20 years ago. Kids who were born during the last decade will never know a world where everyone doesn't have a cellphone on them at all times. They'll never truly understand what the world was like before the Internet.

This rapid development of technology has made it so our kids' online and offline lives are merged into one. The conversations they have on social media or over texting are the exact same as the conversations they would have in person. They have direct access to just about anyone at a moment's notice and can see directly into other people's lives through social media. Additionally, many kids are stumbling upon graphic content and some pop-ups are even encouraging them to click on inappropriate material.

To put it simply, it's becoming much more difficult to keep our children safe online. They're able to share information, pictures and videos at a moment's notice, and oftentimes, the parents are unaware their children are participating in these behaviors. Considering that 40% of American children receive cellphones before they turn 11, it's important that parents do everything in their power to ensure their children stay safe online.

If you're unsure of what steps you need to take to ensure your children's safety online, don't worry – we've got you covered.

Slowly Introduce Digital Media.
Fostering a safe online environment for your children starts at an early age. They should be introduced to the online world when they're

Continued on pg.2

Continued from pg.1

young and taught the safest way to use it. Once they've been introduced to the Internet, set time constraints and do everything you can to ensure their technological devices aren't interfering with their sleep.

Think Before You Post.
Many children will get their first experience with social media thanks to their parents, so lead by example by making appropriate, safe posts that do not reveal personal information. There should be no graphic or mature content on your feed as well, especially if it's public.

Encourage The Use Of Strong Passwords.
Make sure your children know how to create strong passwords as well as the dangers of having a weak password. Teach them to use different passwords for each account and to never share their passwords with anyone outside of the family.

Set Up Parental Controls.
Parental controls are great when it comes to streaming services and computers, but did you know that most smartphones also come with parental controls? On your child's smartphone, you can set parental controls for time limits as well as content restrictions. You can even choose which specific websites they're allowed to visit while blocking everything else. This is a great way to prevent them from stumbling upon inappropriate or harmful content.

The Internet can be an informative and enjoyable place for your children if you take the proper precautions. Teach them the basics of the Internet and preach safety above all else.

> **"40% of American children receive cellphones before they turn 11."**

At Brandon Business Machines, we offer sales and services for the following:

- **Multifunction Copiers**
- **Laser Printers**
- **Managed Print Services**
- **Document Management**
- **Managed IT Services**
- **Cyber Security**
- **Remote Back - Ups**
- **Disaster Recovery**
- **Wide Format Plotters**
- **Shredders and Folders**
- **VOIP Phone Systems**

Organized Cyber Criminals are working together

What is ransomware as a service (RaaS)? You're likely familiar with software as a service (SaaS) but ransomware? What does that mean?

First, let's do a quick recap of what ransomware is. It is a type of malware that holds the victim's files and folders for ransom. Through human error, the malware is deployed and encrypts network data, with a safe return being promised once the ransom is paid. And with payments usually made through cryptocurrency, traceability is eliminated.

The ransomware as a service business model was developed for criminal purposes, with the product or service being purchased for illegal activity. Ransomware requires little effort with potentially big payouts.

However, while ransomware is easy to deploy, it isn't always easy to create. And that's where RaaS comes into the equation. Developers can create the malware once and sell it to multiple cybercriminals. Those crime organizations can then deploy their new attack tool to a large number of users at once. And a resulting ransom can come from a single human error. There's a huge return on investment for all involved, with seemingly little effort.

The business model is structured like many legitimate businesses you're familiar with, but forming a network of organized criminals. On the darkweb you'll find RaaS purchase options in monthly subscription, one time payment, or even profit sharing options that come from successful attacks. And there are even combination offerings of these options. Hackers and cybercriminal operations are highly sophisticated businesses.

You have to take steps to properly protect you and your business against these criminal attacks. Here are a few methods you should be using now.
1. Email Filters to remove malicious links before they reach your inbox.
2. Advanced Threat Protection software on all of your devices.
3. Firewall with malware filtering
4. Educate your users on security awareness to build human firewalls.

Those of us in the IT support business cannot overlook that as we build our efforts to counteract their methods of attack. Be sure to speak with your IT professional to make sure your properly protected against damaging ransomware attacks.

Using Tech To Improve Your Customer Service Experience

Customer service expectations have grown over the last few years, and businesses have had to adapt to meet the needs of their customers. Here are a few ways that tech can be implemented to improve the customer service experience.

For Communication: You can program a chatbot to respond to customers' immediate needs or questions on your website or app.

For Interaction: With the use of augmented or virtual reality, you can demonstrate how a product will look or work for your customers.

For Personalization: Through certain automation programs, you can ensure that your e-mails appear as if they were tailored for each customer.

The Growing Threat Of Ransomware

As the COVID-19 pandemic continues to slow down, technology experts fear that the next major issue to affect our country will come from the digital world. Throughout the pandemic, ransomware attacks have increased 500% and don't seem to be stopping anytime soon.

Ransomware attacks occur when a hacker installs software on a network that prevents the owner from accessing any of their devices or data. They essentially hold the business hostage as they demand a ransom payment. To combat this, your business needs to put some cyber security practices in place to prevent ransomware attacks. This includes implementing offline backups and keeping your software up-to-date.

CartoonStock.c

The Best Tech Helps Attract And Retain Talent

The technology your company uses has always been important in attracting experienced and talented employees, but it has become even more important with remote and hybrid work. Very few employees will want to work remotely for a company that doesn't provide any of the basic tech needed to perform their role. A recent study by Barco, Inc. found that 1 in 3 hybrid employees say that one of the top factors in searching for a new job is their frustration while dealing with tech issues. If you want to retain your top talent, you need to provide your team with the tech needed to perform their daily duties, check on them to make sure they have everything they need and even the playing field between your remote and in-office employees.