



Client Spotlight: Creative Outdoor Advertising

Meet **Creative Outdoor Advertising (COA)**! They have been part of the Connectability client family since February 2018.

Creative Outdoor Advertising has over 37 years of experience in providing StreetScaping programs to over 300 municipalities and transit authorities across North America. They have a solid 30+ year track record and have become the largest advertising company in their segment!

Their products include advertising for street furniture, mainly benches, waste/recycling bins, and transit shelters. Not only do they place signs so that it reaches their clients target audience, they also maintain the advertisements so their signs look brand new all the time.

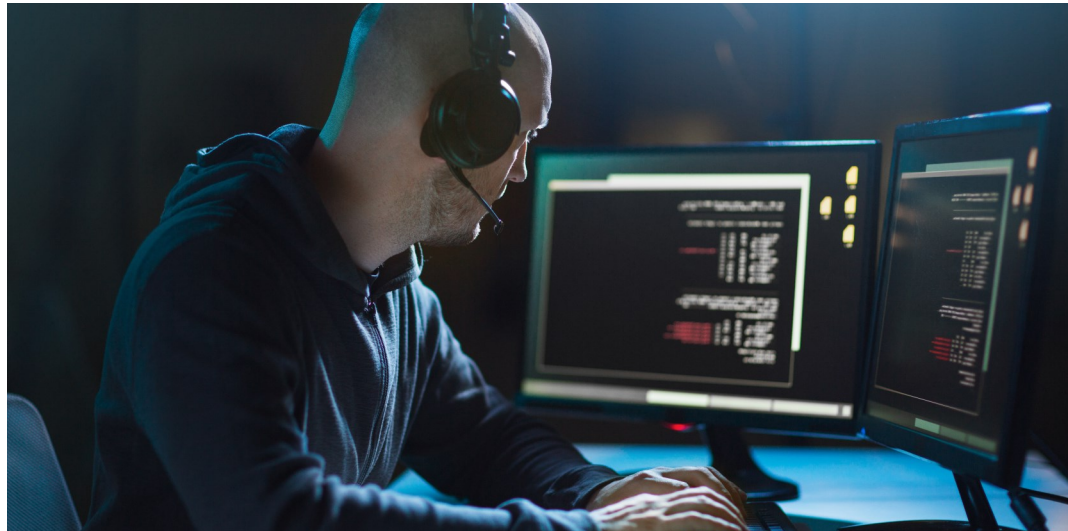
Connectability has been Creative Outdoor Advertising's technology partner for over two years. We monitor their workstations, servers, and backups to ensure they are operating smoothly, and we offer protections to prevent cyber attacks, Ransomware and breaches. We work with their internal IT team to solve technology issues, so that they can focus on finding new customers and servicing existing clients.

If you would like to learn more about Creative Outdoor Advertising, please go to: <https://www.creativeoutdoor.com/>

July 2020



This monthly publication provided courtesy of Ted Shafran, President of Connectability



3 Critical Cyber Security Protections EVERY Business Must Have In Place NOW To Avoid Being Hacked

Five years ago, you might have had state-of-the-art security protecting your business and network. You had the latest malware protection, highly rated firewalls and a great data backup plan. Maybe you even had a handbook on how to address cyberthreats. You were set. But then you forgot to do one crucial thing: you didn't stay up-to-date with your IT security policy.

This is a trap countless businesses fall into. They invest in great cyber security *once*. Five years ago, this was fantastic. The problem is that cyberthreats are constantly evolving. Methods used by hackers and cybercriminals have come a long way in the past five years.

Criminals stay on top of what's going on in the IT security industry. They are always looking for new ways to steal your data and make a quick buck at your expense.

What can you do to stay up-to-date in an ever-changing digital world? Here are three things every business must do to protect itself.

Understand The Threats

It's easy to assume that hackers are trying to get into your network the "old-fashioned" way. You might picture them hacking your network trying to get your passwords and usernames or breaking through your firewall protection. While some hackers will do this (it's easy for them if you use simple passwords), many of today's cybercriminals rely on social engineering.

The most common form of social engineering is the phishing scam. The criminal sends you or your employees an email, hoping someone will click a link or open an attached file.

Cybercriminals have gotten VERY

Continued on pg.2

Continued from pg.1

sophisticated. These emails can mimic the look of a legitimate email from a legitimate business, such as the local bank you work with or another company you buy from (or that buys from you). Social engineering is all about tricking people.

This is why you need a cyber security handbook – one that is regularly updated. It's something you can reference. Your team needs to know how to identify a phishing email, and you need to have procedures in place for what to do if a questionable email shows up. This helps keep your employees from becoming the weak link in your security setup.

Update, Update And Update

From software to hardware, you must stay updated. There is no such thing as “one-and-done” when it comes to network security. Something as simple as a wireless router can DESTROY your security if it's not regularly updated. Hackers are always looking for vulnerabilities in both hardware and software, and when they find them, they WILL exploit them.

What happens when a piece of hardware (like a router) is no longer supported by the manufacturer? This occurs all the time, particularly as hardware ages. Manufacturers and developers drop support for their older technology so they can focus on their newer products. When they drop support for a product you use, this is a good indicator that you need to replace that piece of hardware. The same applies to software.

“Proactive monitoring means your network is being watched 24/7.”

You might balk at the cost of buying new technology, but in the long run, the cost is well worth it. Think of the cost of buying a new router versus the cost of cleaning up after a data breach. Some small businesses never recover after a hack – it's just too expensive. Keep your malware software updated, keep your firewall updated, keep your cloud backups updated and keep all your devices and software UPDATED!

Invest In Proactive Network Monitoring

When it comes to the security of your network and overall business, being proactive can make a huge difference. Proactive monitoring means your network is being watched 24/7. Every little ping or access to your network is watched and assessed. If a threat is found, then it can be stopped.

The great thing about proactive network monitoring is that you can customize it. Want to know about every threat? You can request a real-time report. Only want updates once a day or once a week? That can be done too! This approach means you have one less thing to think about. Someone is always keeping an eye on your network, making sure the bad guys stay out.

You might think, “How am I going to do all this?” You don't have to go it alone – and you shouldn't. Work with an IT services firm. Work together to find the best solutions for your business. When you work with IT specialists, you can rest assured your team will be updated on today's threats. You'll know your network – and everything connected to it – is updated. And you'll know someone is watching over you. That's the ultimate peace of mind.

Quick Tip: Secure Your Cloud Applications

If you're using cloud applications while your employees are working from home, you are right to be concerned about data privacy and security. The company hosting your data is ultimately responsible for keeping hackers out of THEIR network, but most cloud breaches are due to USER ERROR.

Here are a few things you can easily do to improve security in the cloud:

- Maintain a STRONG password of at least eight (8) characters with both uppercase and lowercase letters, numbers and symbols. Do NOT make it easy, such as “Password123!” While that technically meets the requirements, a hacker could easily crack that.
- Make sure the device you're using to access the application is secure. You'll need professional help installing and maintaining a strong firewall, antivirus and spam-filtering software. Don't access your cloud applications with a device you also use to check social media sites and free email accounts.
- Back up your data. If the data in the cloud is important, make sure you're downloading it from the application and backing it up in another safe and secure location. If your account gets hacked OR if the cloud company shuts down your account, you have a copy.

If you're concerned about the security of your cloud applications or if you have any other IT questions, please call us at (647) 492-4406.

Shiny New Gadget Of The Month:



Drone X Pro

People are constantly looking for creative ways to express themselves, document their daily lives, share their adventures with their loved ones, and immortalize the most precious memories...

Nowadays, it's not so easy to stand out from the crowd, but there's finally one assured way to do it – and we call it DroneX Pro!

DroneX Pro was created with simplicity in mind so that everyone could use it. There's no need for heavy, bulky devices anymore – DroneX Pro's well-thought-out and ultra-compact design allows you to carry it wherever you go since it can easily fit in your pocket!

Despite the DroneX's size and portability, it provides you the most valuable features of high-quality drones and turns the process of taking pictures into an incredibly fun and entertaining experience!

Communicate and Stay Connected with VoIP

Due to the pandemic, a lot of things are up in the air right now. And because businesses have moved to a remote work model, communication with your partners, team, clients, vendors, and so on, is more important than ever. Having a dispersed workforce can make staying connected to your clients and partners a challenge for many businesses. A VoIP phone system can help.

Voice over Internet Protocol (VoIP) uses the internet to make and receive phone calls. VoIP allows you to communicate with your stakeholders in the manner they've grown accustomed to, but that's not all. Here are 3 benefits of VoIP you can leverage during these unprecedented times.

- 1. Great for Remote Work Environments**
 VoIP systems can be heavily customized. If for example, you want your office phones to ring from 9 am – 5 pm, but after 5 pm you want it directed to a cell phone, you can do that. VoIP is also great for remote employees. They can use company owned handsets from home as if they are in the office, or if you don't want your employees taking company-owned equipment off-site, they can download an app that acts as an office phone. As long as your employees have an internet connection, your phone system will work!
- 2. Improves Functionality**
 It's very difficult to manage a traditional phone system in a remote work environment. You can forward your number to a cell phone, but how do you

transfer calls? Well, VoIP systems allow you to pick up calls, transfer them to your colleagues, and direct people to a voicemail box if necessary. Additionally, you can take advantage of a feature called voicemail to email that automatically saves all voicemails as audio files and sends them to you via email, that way you get the message regardless of your location.

- 3. Reduces Costs**
 Everyone is looking for ways to reduce expenses right now, and a VoIP system is an easy way to shave some cost. Most VoIP systems have no monthly contracts, so all you need to worry about are call charges, and the fee from your IT provider to manage the system. And because call charges are very low, we find that our customers reduce their phone bill by, on average, 75% when they switch from a traditional phone system to VoIP. Plus, you don't need phones to make this solution work – all you need is a computer (or cell phone) and an internet connection. VoIP also allows you to scale up or down depending on the number of lines you need for your business.

If you want to reduce costs, improve communication, or if you need a tool for your dispersed workforce, then VoIP might be the answer. Call us today at (647) 492-4406 and we can discuss your organization's needs and help set up a VoIP solution.

Tech Connect Video Series: Password Security Is No Joke!

The best way to keep a bad guy from entering your home or workplace is through a robust security system. These systems can prevent a criminal from getting in and stealing your valuables, such as your passport, financial documents, photos, equipment, and much more. Imagine the frustration a break in would cause?

The same thing can also happen online. A hacker can access your systems and steal your confidential information. They can rummage through your financial statements, customer lists, and personal emails. That's why password security is so critical—it's the first lock on your digital "door". Unfortunately, a lot of people use the same passwords for their email, online banking, computer, Facebook, and Amazon, making it easy for a hacker to get in. All they need is one password.

If you'd like to learn more about protecting your passwords and preventing cyber criminals from accessing your accounts, watch this video NOW! You will learn 4 simple ways to secure your passwords. To find out more, go to **YouTube**, look up **Connectability IT Support** and find the video **"4 Simple Ways To Secure Your Password"** OR go to our website at **www.connectability.com**, hover over **"Resources & Videos"** and select **"Videos"**.

■ 3 Technology Truths For Transforming Your Business

1. You have to keep up. Tech changes fast. By the end of this year, 5G will be more widely available – along with devices that can use it. More businesses will be relying on artificial intelligence to supplement productivity and customer interaction, putting them light-years ahead of the competition that lags behind.

2. You have to invest. Change comes with cost. If you aren't willing to invest in new tech, then you will fall behind, and so will your support and security. If you run into any problems, then you could be in big trouble.

3. Don't fall behind on cyber security. It's easy to forget about

cyber security when things are running smoothly and working as intended. But cybercriminals never stop. They are always looking for a way in, and if you fall behind the times on your IT security, then you make it easier for them. Keep your data and your customers as secure as possible. *Inc., July 30, 2019*

■ How Malware Can Cripple Your Business

Every year, the number of malware attacks on small businesses increases. Symantec's 2018 Internet Security Threat Report found that between 2017 and 2018, malware increased by 54%.

The term "malware" covers a number of different malicious programs, including ransomware, spyware, viruses, worms, Trojan

horses and more.

In many cases, malware is designed to take over your computer. It may be programmed to look for specific data or it may give a hacker remote access to your files. In the case of ransomware, it locks you out of your computer until you pay the hacker a ransom. After that, the hacker may give you back control – or they might delete everything on your hard drive. These are not good people.

If you don't invest in cyber security, then hackers can destroy your business. It's already happened to countless businesses across the country. It's estimated that websites experience up to 58 cyber-attacks every day. Protect yourself before it's too late. *Small Business Trends, Oct. 12, 2019*

"My password is 'again'. Whenever I forget my password, the computer message says 'Try again'."



SickKids®

This month we will be donating to the **Cochlear Implant Program at SickKids Hospital.**

Founded in 1900, the Cochlear Implant Program is one of the largest paediatric centres for cochlear implantation in North America. Approximately 1500 children have received cochlear implants. The program helps children who suffer from hearing loss to receive implants that will help develop their speech and language.

The Cochlear Implant Program has a designated team of 16 individuals, and a close association with Archie's Lab at SickKids. The laboratory conducts research on plasticity and the development of auditory systems. Additionally, a centre has been created to explore and understand how children with cochlear implants interpret sound.

If you want to contribute to the Cochlear Implant Program at SickKids Hospital, we would love your help! Email: info@connectability.com or call (647) 492-4406.