Centrend
Volume 6.0
Monthly Newsletter
THE TECH CHRONICLE
September 2023 www.centrend.com Friday

What's Inside?

Product Spotlight

The Top Five Reasons for a Slow Network (and How to Fix It)

We've all experienced that frustrating moment when our internet network starts crawling at a snail's pace. It can be incredibly annoying, especially in today's interconnected world, where we rely on the Internet for work, communication, entertainment, and much more.

When your internet network gets slow, it disrupts your productivity and interrupts your online activities. Whether you're trying to load a webpage, stream a video, or download a file, the waiting time feels like an eternity. It's not only irritating but also time-consuming.

The annoyance grows even more when you're in the middle of an important task or engaged in an exciting online game. The lag and delays can ruin the experience and leave you feeling frustrated and powerless.

In this fast-paced digital era where we depend heavily on a smooth internet connection, experiencing slow network speeds creates an unwelcome disruption to our daily lives.

>>> continued on Page 2

CONCEALBrowse™

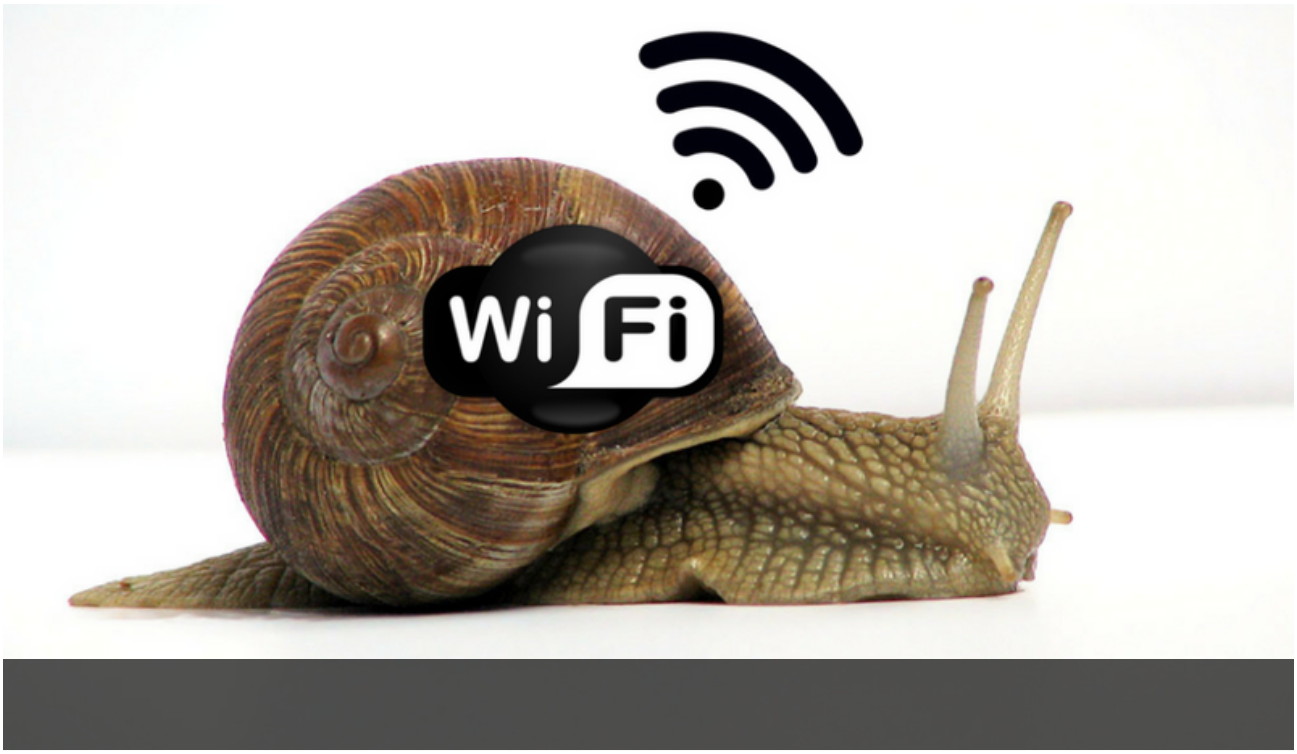
Your Ultimate Comprehensive Browser Protection

Picture this: you're browsing the internet, searching for information, or making online transactions, oblivious that your personal data and sensitive information are at risk. How frightening is it to not know if the browser you're visiting is not secured? In today's digital age, where cyber threats are becoming increasingly sophisticated, ensuring the security of our online activities has never been more critical.

>>> learn more on Page 7

Jeff Orloff
VP Product and Customer Experience

The Top Five Reasons for a Slow Network (and How to Fix It)



It hampers our ability to stay connected with loved ones, complete work assignments efficiently, or enjoy browsing the web hassle-free.

Thankfully, there are steps you can take to improve your internet speed and reduce that annoying feeling when your network gets slow. From troubleshooting basic connectivity issues to optimizing router settings or considering an upgrade from your service provider, solutions are available to help alleviate this common frustration.

Inadequate bandwidth

Overloaded bandwidth brought on by congestion is the most frequent cause of a slow network. A bottleneck causes customers to suffer delays and slow traffic when the total amount of data demanded by all users exceeds the network service's capacity.

A webpage can load slowly, or a download might crawl at what feels like dial-up speeds, for instance, if everyone is using the internet service provider's capacity simultaneously while the user tries to access the Internet.

How can this issue be solved? The best course of action will need to be chosen once the precise reason for a bandwidth issue has been identified, whether it be an ISP service or a network component. There may be ways to lower consumption during such times of the day if the bottlenecks only occur during peak hours. It's time to upgrade if network usage has surpassed the allocated bandwidth. The issue can be resolved with a new agreement with the ISP or by purchasing more network hardware.

Noise and Interference with Wireless Signals

Signal interference is another frequent cause of a wireless connection that is slower than usual. Wi-Fi access points must be carefully positioned and set to prevent interference.

Data packets are frequently dropped during interference, forcing the device to seek the same data repeatedly. The user encounters a sluggish connection or one that appears to function only occasionally.

Other gadgets that produce noise on the same frequencies as Wi-Fi devices can cause interference. When operating, microwaves and the electric motors that drive cleaning equipment have been found to interfere with Wi-Fi signals.

How can this issue be solved? Have IT support personnel determine whether the access points need to be modified if slow connections only occur when using Wi-Fi in specific office areas.

Configuration of Network Devices

Sometimes, the setup of the machine being used is the cause of a poor network connection. There's a good possibility that the device and not the network are to blame if no other nearby users are complaining about poor connections. A configuration mismatch between the network and workstation can result in issues if the workstation is new or the network has just undergone changes. If the computer is outdated, its hardware might need to be upgraded to utilize the entire available network bandwidth.

How can this issue be solved? When workstations and mobile devices are first distributed to consumers, they must be properly set up. IT administrators should assess any modifications required in the network devices when upgraded or modified. A specific device will need to be troubleshooted by network support personnel when these issues arise. A quick software update might resolve the problem, or the hardware might require a network card upgrade.

Internet Service that Isn't Reliable The Internet service provider may also be to blame for a slow Internet connection. Although Internet service is often dependable, several things can happen between the distance between an ISP's headquarters and its clients. There could be actual infrastructure improvements being made by the ISP or a downed upstream transmission line. The issue might be a configuration problem, which the ISP's support staff can quickly resolve when alerted.

How can this issue be solved? The next place to look is the Internet service provider if there are no issues with the local network and most or all Internet customers are experiencing a slow connection. Ask their support team if they know of any network congestion problems or slow, poor line conditions and if anything can be done to resolve them.

Malware Infection

Slow network connectivity might also be a result of malware infection. Adware is malware that frequently infects workstations, adding to the network burden and degrading web browser performance. Malware can damage a device's operating system or occupy its CPU. Malware can infect switches, routers, and workstations in a corporate network. Adware and data exfiltration software are two examples of malware that can infiltrate office networks and steal enormous amounts of data.

How can this issue be solved? Unless a significant amount of data is transferred, malware often only causes enough network congestion to delay connections across the network. Typically, it only becomes apparent on isolated workstations when performance issues arise. Contact IT Support immediately when there is a suspicion of a malware infection. It can signal that the network is compromised or that additional workstations are infected.

Remember that a reliable and fast internet connection is essential for seamless productivity and enjoyment in today's connected world. Take control of your online experience by proactively addressing any network speed issues – say goodbye to that frustrating feeling of dealing with slow internet networks. Book a **FREE 10-minute** consultation with us today and learn how we can quickly get you back up to speed!

Common Cybersecurity Issues that Organizations Face

In today's digital age, cybersecurity has become the top concern for individuals and organizations. With the increasing reliance on technology and the growing number of cyber threats, it is crucial to prioritize protecting our sensitive data.

The high-risk vulnerabilities in our digital infrastructure make cybersecurity issues even more pressing. Hackers are constantly finding new ways to exploit weaknesses in systems, making it imperative for us to stay one step ahead.

As the technology landscape continues to evolve, the importance of cybersecurity grows exponentially. It is not just a problem for big corporations or governments; individuals also face significant risks regarding online security.

The following are several cybersecurity issues and threats to be aware of in today's business landscape. Social Engineering (Phishing Attacks.

It is considered to be the most significant, most damaging, and the most widespread threat among small and medium businesses.

Based on the studies, ***90% of all the breaches*** that organizations encountered grew to 65% over the previous year, equating to ***over $12 billion in business losses/damages***. From a simple tactic of pretending to be a trusted source and enticing victims to click, download, or provide access to personally sensitive information and confidential details to being more sophisticated, that makes it challenging to combat.

Malware Attacks

Malware Attacks are the second most prominent and most damaging threat in business. These attacks target business devices that will cost you a lot of financial resources to repair, replace, or fix. Malware usually comes from malicious website downloads, spam, or from other infected machines or devices.

Most of these attacks use email or corrupted websites to penetrate the system and make a network vulnerable. Such attacks leave business owners and decision-makers with a challenging choice. Decide to pay the ransom demanded by the attacker or recover from backups **if backups were not corrupted.**

According to reports, 71% of ransomware attacks target small businesses with an average ransom of $116,000. The healthcare industry is the most impacted sector, as it has one of the most highly protected categories of information – patient medical records. In this case, the risk is not just data loss. The attackers also threaten to publish their stolen information, leading to severe **HIPPA** fines.

Weak Passwords

Another major threat that business owners are facing nowadays is users with weak passwords. Like any other business organization, everyone uses and needs multiple cloud-based services that mostly contain personally sensitive, financial, and confidential information. According to studies, most businesses are using easily

guessed passwords or even share passwords with a lack of overall regarding the risk created by the practice.

Artificial intelligence (AI) and machine learning (ML)

Artificial intelligence (AI) and machine learning are tools that cybercriminals can use to increase the sophistication and effectiveness of their attacks. Both are valuable tools for criminals since they may "learn" which attack strategies are effective and which are not. Fortunately for knowledgeable cybersecurity workers, cyberattacks can also be thwarted using AI and machine learning.

Crypto and blockchain attacks

Cryptocurrencies and blockchain technologies are increasingly being used in business. The global cryptocurrency market (hardware, software, platforms, and services) is anticipated to hit around $5 billion by 2030, according to a survey by Allied Market Research. Due to the sluggish development of the infrastructure required to protect the information linked with these assets, this digital trade has become a haven for cybercriminals. Those intending to employ blockchain in their companies should exercise extreme caution to ensure their cybersecurity plans cover these new, developing markets.

Third-party software

Small businesses are a desirable target for online attackers. One explanation is that their more compact computer networks occasionally serve as entry points to larger targets. Small businesses frequently need more effective security measures to deter theft. The 2013 Target hack is a well-known instance of this kind of attack. The initial cyber-attack on a tiny company that provided HVAC maintenance for Target was where the attack first started. About 40 million credit and debit card numbers and about 70 million personal records, including sensitive data, were ultimately stolen due to this incident.

Amidst this challenging landscape, fostering a culture that prioritizes cybersecurity at all levels - individuals to businesses and governments is essential. By working together and taking collective responsibility, we can create a safer digital environment for everyone. Book a **FREE 15-minute call** with us to learn more about how we can effectively protect our digital lives.

Remember: Cybersecurity matters. It's time for us all to take action and protect what matters most – our data!

What Business Owners Can Learn from Data Breaches

The cost and impact of data breaches cannot be overstated in today's digital landscape. With the increasing reliance on technology and the vast amount of sensitive data being stored and transmitted, businesses are more vulnerable than ever to cyber-attacks.

Data breaches can have severe financial consequences for organizations. Companies face immediate costs such as investigating the breach, notifying affected individuals, and implementing security measures, and they also suffer long-term financial losses. These losses can include legal fees, regulatory penalties, loss of customer trust, damage to brand reputation, and even potential lawsuits from affected parties.

To mitigate the cost and impact of data breaches, businesses must invest in robust cybersecurity measures such as encryption protocols, network monitoring systems, employee training programs on data security best practices, and incident response plans. Proactive steps like regular security audits and vulnerability assessments can also help identify potential weaknesses before malicious actors exploit them.

Here are the key takeaways of business owners with the most recent and most famous breaches across the globe:

1. Be the leader and be involved in the decision-making process.

With the progressing number of cyber-attackers, business owners, executives, and decision-makers have become more invested and involved with implementing solutions or workarounds whenever an attack occurs. According to the study, 54% of the executives and 39% of the company's directors are in the loop and knowledgeable in the planning stage of the practices and responses to cyber-attacks and data breaches. The engagement of C-suite executives is as crucial as it may seem, as it shows that the organization is serious about protecting its client's data.

2. Train your workforce

According to reports, 47% of data breaches were caused by human mistakes/negligence, accounting for an average of $5 million in business losses. Proper training in security awareness and highlighting its importance on a business entity is a huge help to lessen or mitigate the probability of human error and strengthen the practice of digital hygiene.

3. Plan a Disaster Recovery Plan

It takes an average of 279 days for a data breach to be detected in an organization's system – that equates to over nine months. That said, it is a MUST that a business has a Disaster Recovery Plan or Business Continuity Plan in preparation for the worst-case scenario. Being complacent and thinking that only giant corporations are attacked by cybercriminals is one of the myths in the digital space nowadays. 93% of companies without disaster recovery plans suffer major data disasters and financial losses and face bankruptcy within a year.

So, it is imperative to have a secured cloud backup that allows the business to recover its most essential data, applications, and even configurations. Remember, a disaster recovery plan must always be on top of your cybersecurity agenda to help you quickly bounce back from any possible crisis and attack.

4. Cybersecurity is an investment and an ongoing process

As cybercriminals become increasingly sophisticated in their ways, Cybersecurity and preventive measures of business should be a continuous process, too. Ongoing assessments of the company's capabilities during any possible attacks must be done as the cybersecurity landscape constantly changes from time to time. Every business organization, regardless of its size, should constantly update its security policy, continuously improve existing systems and functions, and implement new processes that fit into addressing the company's vulnerabilities.

In conclusion, the cost and impact of data breaches are high-stakes issues that require immediate attention from businesses across industries. By prioritizing cybersecurity measures and implementing preventive strategies, organizations can minimize their vulnerability to attacks and protect themselves from devastating financial losses and reputational damage.

Learn more about Cybersecurity and get a **FREE 10-minute assessment** by clicking the link below.

ConcealBrowse: Your Ultimate Comprehensive Browser Protection

In a world where we rely heavily on technology and spend a significant amount of time on the internet, the issue of online security cannot be underestimated. The potential consequences of accessing an unsecured browser are alarming – from identity theft and financial fraud to unauthorized access to personal information. As users, we must understand the risks of using unsecured browsers and proactively protect ourselves.

Moreover, unsecured browsers may leave us vulnerable to malicious software or malware that can invade our devices and compromise their functionality. These threats can lead to system crashes, loss of important files, or even allow hackers remote access to our devices for nefarious purposes.

Beyond these immediate concerns, long-term implications exist for businesses and organizations that fail to provide secure user platforms. The loss of customer trust due to a lack of security measures can severely affect brand reputation and customer loyalty.

Thankfully, we have discovered Conceal IO's Conceal Browse - which creates a safe and secure way for every user to browse the internet by proactively detecting and blocking potentially malicious URLs that could be used to execute attacks on your employees' devices

ConcealBrowse was developed due to the enormous web browser attacks as cybercriminals get sophisticated with the ways they can exploit.

According to studies, 80% of employees spend 80% of their time with their web browsers – this equates to higher chances of becoming vulnerable to cyber-attacks. Business organizations consider web-based attacks as one of their biggest security challenges, aside from phishing, malware, smithing, and slinking, which mainly target employees' work applications.

ConcealBrowse was created to provide comprehensive browser protection for businesses and individuals to mitigate these growing threats.

What is ConcealBrowse?

ConcealBrowse is a lightweight browser extension that converts any browser into a ZeroTrust, secure browser that detects and prevents malware, such as ransomware, and credential theft attacks that bypass other security controls. It protects endpoints and users from malicious, unknown URLs by analyzing metadata signals in the content of a web page and its URL. When the extension determines that something is suspicious or unknown, ConcealBrowse intervenes and sends the user's browser to a protected state that allows them to visit the page in a web-based container that protects them from any potential malicious activity. ConcealBrowse outright blocks known malicious sites as a layer of protection, while known 'good' URLs can continue down their normal path. It makes proactive decisions about the security risk associated with internet use and automatically intervenes to offer the appropriate level of protection against any potentially risky transactions.

We have interviewed Jeff Orloff – Vice President of Product and Customer Experience for Conceal IO, makers of ConcealBrowse, to learn more about the fantastic features of their zero-trust browser security tool.

We've asked Jeff what makes ConcealBrowse unique from the existing competition in the market. According to him, traditional browser isolation solutions often rely on full-time browser isolation to keep users in a protected state at all times. This poses several issues for the end user. It leads to slower loading times, hindered multimedia delivery, and even malfunctioning business-critical applications. The technologies used in these solutions are the root cause of these experience issues. Other solutions opt to force the users to install their secure browser solution. Organizations must remove and replace existing browsers with the vendor's secure offering. The user experience suffers because they want to use their preferred browser. Changing browsers and forcing constant isolation is costly and requires a great deal of change management and training in the organization.

Also, when people find that they can't get their work done due to the constraints posed by these solutions, they often look for ways around them. This causes further security controls and limits to be put in place. ConcealBrowse overcomes these limitations, offering an optimized user experience alongside robust protection at an affordable price point. Unlike other browser isolation solutions, ConcealBrowse, powered by the ConcealSherpaAI engine, identifies suspicious sites before isolation, resulting in an unintrusive, seamless user experience.

Mr. Orloff explains, ***"We are solving the problem of web-based threats. There are too many attack vectors in which malicious links can be put in front of a potential victim. ConcealBrowse looks to fill a need for anyone who works through their web browser."***

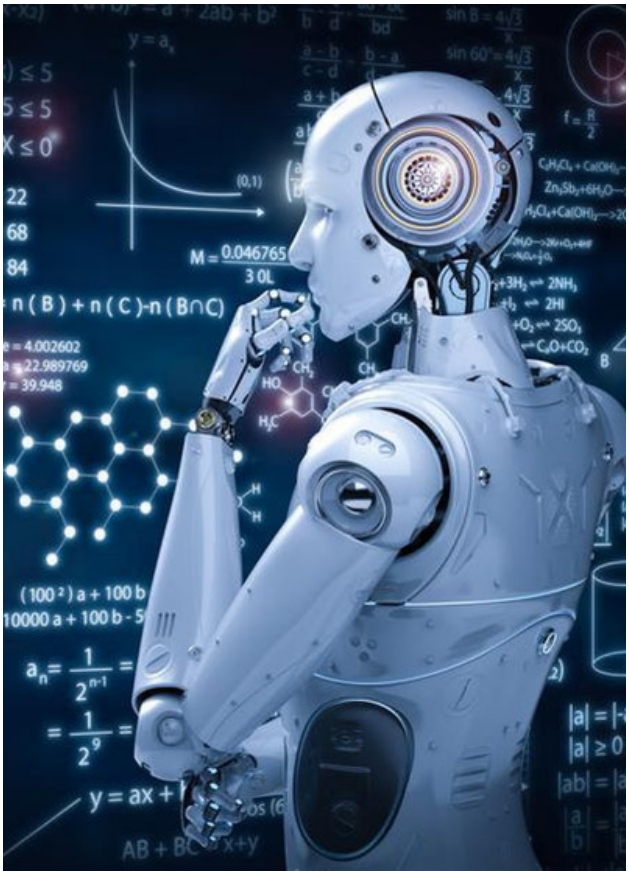
Mr Orloff explains that compared to other solutions that only depend on URL analysis, ConcealBrow***se delivers a higher level of danger prevention. "We can detect and prevent prospective threats using ConcealBrowse's SherpaAI by allowing it to recognize novel patterns in enemy strategies and methods. "***

Centrend has discovered that ConcealBrowse is a straightforward system to implement as part of a cybersecurity preventive action. In addition to being reasonably priced, the extension works in just a matter of minutes with no configuration necessary.

It is crucial to keep our browsers updated with the latest security patches and use reputable antivirus software that safeguards against potential threats. Additionally, being mindful of the websites we visit and avoiding suspicious links or downloads goes a long way in preventing security breaches. Diligence is not enough. Malicious hackers sneak code into some of our most trusted resources on the web.

ConcealBrowse should be a vital tool in your cybersecurity layer. At only $2 per device per month, it's extremely affordable to acquire whether you have one computer to protect or dozens of devices. Investing in your online security by adding ZeroTrust to your browser is essential to safeguarding your personal information. Don't let fear paralyze you - take control of your online safety today and enjoy a worry-free browsing experience! Schedule a **FREE** consultation on how ConcealBrowse fits your device protection strategy.

The *Future* of Cybersecurity



As we progress further into the modern world, the importance of cybersecurity continues to grow exponentially. With technological advancements and increased digital connectivity, the future of cybersecurity is more crucial than ever.

In this rapidly evolving landscape, more than traditional cybersecurity measures are required. Hackers are becoming more sophisticated, targeting individuals and organizations with highly targeted attacks. As a result, we must look towards the future of cybersecurity to stay one step ahead.

The future of cybersecurity lies in cutting-edge technologies such as artificial intelligence (AI), machine learning (ML), and quantum computing. These technologies can potentially revolutionize protecting sensitive information and staying safe in an increasingly digital world.

AI can play a vital role in identifying and neutralizing threats by analyzing vast amounts of data for patterns and anomalies. ML algorithms can continuously learn and adapt to new threats, making them invaluable tools for staying ahead of cybercriminals.

Furthermore, quantum computing can significantly enhance encryption, rendering current hacking techniques obsolete. With quantum-resistant algorithms, data encryption will become virtually impenetrable even to the most advanced hackers.

Here's what the future of cybersecurity will look like:

Increase rate of ransomware threats

Ransomware attacks are expected to increase and become dominant as the years go by. The trend will continue to rise with more significant attacks and devastating impacts on business organizations, especially their financial resources. With the constant technological evolution, cybercriminals will use it as a catalyst to find new weaknesses and flaws to exploit.

Challenges to secure remote access

With the recent changes in the work set-up of most remote employees, cyber attackers continue to develop a more sophisticated way of finding ways to target employees connected to a corporate network while working from the comfort of their homes.

An army of cyber experts

The need for cybersecurity experts has grown by 60% since 2020. The COVID-19 epidemic sparked hyper-digital shifts across numerous businesses. There is a greater risk of cyber-attacks as more data and sensitive information is shared online or in the cloud, necessitating the hiring of additional experts who can address the changing cyber landscape.

Quantum Computing to Prevent Fraud

Quantum computers perform operations at exponentially quicker rates and with significantly less energy consumption than conventional computers, which are constrained in their processing capabilities. Quantum computers are helpful for complex cybersecurity applications because of their agility.

Cryptography

Cryptography is one of the most intriguing applications of quantum computing in cybersecurity. It entails converting data or communications into a code while keeping the message from being understood by unauthorized persons, even if they intercept it. Researchers are developing quantum-resistant cryptography to stave off attacks from quantum computers.

Cryptography has many uses, from protecting financial transactions to facilitating secure communication between people or organizations. It is necessary to protect sensitive data from hackers and other bad actors.

Cybersecurity experts must upgrade their skills as new technologies like blockchain, quantum computing, and AI develop. While utilizing these technologies for protection measures, cybersecurity engineers, analysts, and architects must know how new technology can be used for more sophisticated cyber-attacks.

Blocking Crime Using Blockchain

Although cryptocurrencies like Bitcoin and Ethereum are where blockchain technology is most commonly used, there are many applications outside of cryptocurrencies.

Blockchain may create a secure and impenetrable record of transactions and data exchanges, a significant benefit for cybersecurity. Businesses can create a transparent and reliable system for recording and confirming data transactions by recording unchangeable transactions. This system can be beneficial in supply chain management and identity verification.

Another blockchain technique for cybersecurity is smart contracts. Self-executing contracts, known as "smart contracts," are those in which the terms of the buyer-seller contract are written directly into the code. These could be used to pay staff every Friday, to register a car after buying it, or even for other purposes. Learning continues to advance in this modern day, and humans will have difficulty discerning computer-generated transactions from people-generated transactions. However, with incredible advancements also come significant challenges. As cyber threats evolve, so too must our approach to combating them.

Collaboration between governments, private sector organizations, and individuals will be essential for developing robust cyber defense strategies that protect us from emerging threats.

Ultimately, as technology continues its relentless innovation in the modern world, so do the challenges posed by cybercriminals. Embracing AI technologies such as machine learning and quantum computing will form a crucial part of our future defenses against these ever-evolving threats. By leveraging these advancements and collective efforts across sectors, we can usher in a safer digital landscape for future generations.