

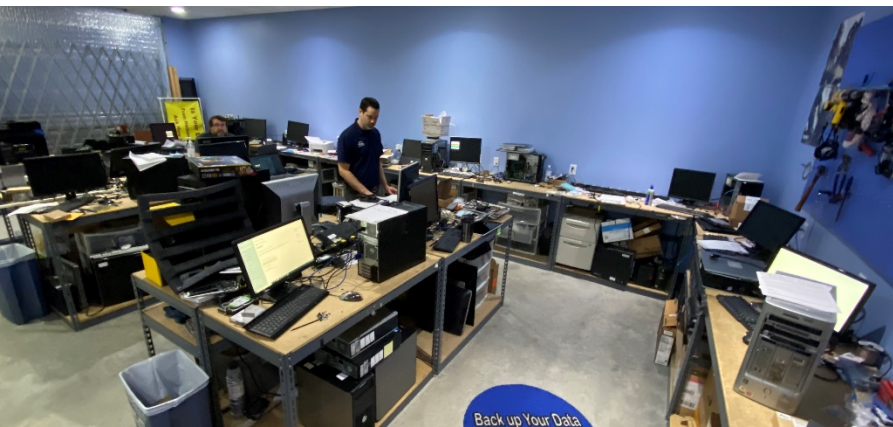


**IMPRESS**  
COMPUTER SOLUTIONS

12 Essential Security Basics  
Every Business Owner Should Know

# History Of Impress Computers

- Roland and Mandy Parker formed Impress back in Zimbabwe in 1994
- They grew the company to one of the largest IT firms in the country
- In 2003 they made the move to Katy TX
- Over the past 18 Year Impress Computers has become a well known name in the community, with hundreds of 5 star reviews and many customers have been with us since the beginning





# The Cost of Falling Victim

Ransomware attacks are constantly making news headlines. However, the stories you hear often focus on large enterprise organizations. Today, cybercriminals frequently target small to medium-sized organizations, which are often more vulnerable to these attacks. Additionally, ransomware attacks can destroy a business as a result of the financial burden inflicted from direct and indirect damage. In addition to the ransom payout, you must factor in downtime, reputational damage, data loss, and other repercussions that may follow.



2020

## Average

In 2020, the average ransom demand for SMBs was about \$312,493. However, this does not factor in the downtime and damages that follow. The average cost of downtime in 2019 for SMBs comes out to \$141,000, a 200% increase over the previous year's average downtime cost of \$46,800.



## Compromised Data

On the dark web, the average cost of a medical record is about \$400, which is 2.5x times the average of overall industries. Victims who have their medical records compromised are often left grappling with the effects years later.



## Recovery Time

As of January 2021, the average number of days a ransomware incident lasts is now 18 days. This is a result of the time needed to remediate and restore systems after an attack.



## 60 Percent of Small Businesses Fold Within 6 Months of a Cyber Attack.

- 60 Percent of Small Businesses Fold Within 6 Months of a Cyber Attack.
- A significant data breach can ruin a company's reputation and even drive it to bankruptcy. Stricter government regulations also dictate how electronic information must be stored and secured. Considering all this, the role of IT security has become more important than ever.



## What is Ransomware?.

- Type of Malware that infects your computer and then encrypts all your data, making it unusable until ransom is paid (but no guarantees!)
- Recent events have seen an increase in double-extortion where victims data is sold on the dark web
- Normally spread through clicking on attachments or links in emails, or embedded in PDF's, Spreadsheets, Word Docs etc



# 1. Employee Training

- One low-cost option that organizations should adopt immediately is education. Both current employees and new hires should be exhaustively schooled in recognizing a cyber attack and reacting properly. Quick thinking in the early stages of an attack can prevent it from turning into the kind of breach that kills a business.
- Some common items that should be taught:
  - Scam Emails
  - If they suspect foul activity to let IT know ASAP
  - Keeping Password Safe



## 2. Rapid Reponse

- **Ransomware Spreads like WildFire**
- **Train your employees to be on the look out for signs of Ransomware**
- **Disconnect Computer from the network and shut it down as soon as you can**



# 3. Firewall's and Open Ports

## Firewall

- A firewall is a network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules.
- Main Risk of Not Having a Firewall:
  - You don't click on unknown links or attachments.
  - You only log on to trustworthy, known websites.
  - You never give out any personal information unless it is absolutely necessary.
  - You have strong, unique, complex passwords for each online account that you update often.
- Without a firewall, you're accepting every connection into your network from anyone.

## Open Ports

- Be on the lookout for Open Ports on your Firewall
- Open ports become dangerous when legitimate services are exploited through security vulnerabilities or malicious services are introduced to a system via malware or social engineering, cybercriminals can use these services in conjunction with open ports to gain unauthorized access to sensitive data.
- Exploiting vulnerabilities in services and applications running on open ports
- Spreading malware infections through open ports



## 4. Anti Virus, Anti Malware

- Keeping your Anti Virus and Anti Malware Subscription up-to-date is an important 1<sup>st</sup> line of defense against Ransomware, and it is great for preventing known ransomware from running
- However it cannot stop it once it has taken control of your system
- You can no longer rely on just having Anti Virus software



# 5. Multi-Factor Authentication

- Authentication using two or more different factors to achieve auth.
  - Factors include
    - Something you know (password/PIN);
    - Something you have (e.g., cryptographic identification device, token);
    - Something you are (e.g., biometric).
- Cybercriminals have more than 15 billion stolen credentials to choose from. If they choose yours, they could take over your bank accounts, health care records, company secrets, and more.
- Multi-factor authentication is important, as it makes stealing your information harder for the average criminal. The less enticing your data, the more likely that thieves will choose someone else to target.
- Risk reduction is critical for organizations, which is why multi-factor authentication is growing exponentially. In a world where credential harvesting is a constant threat and over 80 percent of hacking-related breaches are caused by stolen or weak passwords, this kind of bulletproof authentication solution is essential.



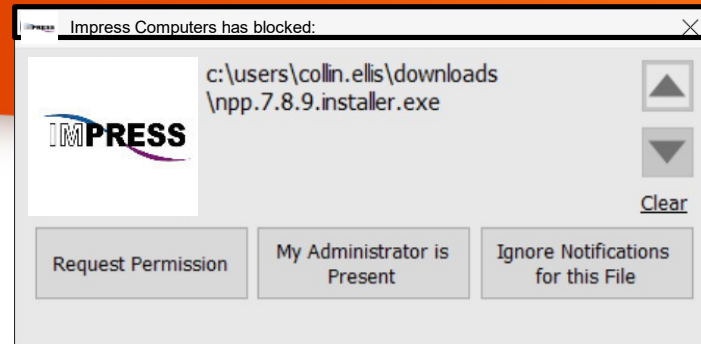
## 6. Email Security

- Preventing **ransomware** requires a multi-layered approach to **security**. In addition to a strong firewall and antivirus software, you can block **email** containing **ransomware** by using content scanning and filtering. Maintaining an archive of **email** and file data helps to eliminate data loss should your servers become infected



## 7. Zero Trust Policy-Driven Security

- Zero Trust is a security concept that requires all users, even those inside the organization's enterprise network, to be authenticated, authorized, and continuously validating security configuration and posture, before being granted or keeping access to applications and data.
- This added layer of security is critical as companies increase the number of endpoints within their network and expand their infrastructure to include cloud-based applications and servers.
- The case of Edward Snowden demonstrates the importance of why organizations can't drop their guard with approved internal users. As a subcontractor for the NSA, Snowden had the appropriate credentials to access the network.
- Had Zero Trust and the principle of least privilege been in place, Snowden's activities would have been more easily discovered, if not outright prevented.



The approval center allows Impress Computers to easily control what is permitted to run on your computer with a 30-second single click approval.

Users have the ability to request permission or ignore notifications for unapproved applications.



## 8. Ring Fencing

- Ringfencing builds fences around applications to define how they can integrate with other software, files, network or registry resources
- So if a white listed program gets compromised, Ring Fencing will prevent it from doing anything malicious



## 9. Backup Backup Backup

- The purpose of the backup is to create a copy of data that can be recovered in the event of a primary data failure.
- Primary data failures can be the result of hardware or software failure, data corruption, or a human-caused event, such as a malicious attack (virus or malware), or accidental deletion of data.
- Backup copies allow data to be restored from an earlier point in time to help the business recover from an unplanned event.



## 10. Staying Current in the IT World

- The truth is it's easy to skip software updates because they can take up a few minutes of our time, and may not seem that important. But this is a mistake that keeps the door open for hackers to access your private information, putting you at risk for identity theft, loss of money, credit, and more.
- In fact, many of the more harmful malware attacks we see take advantage of software vulnerabilities in common applications, like operating systems and browsers.
- In addition to security fixes, software updates can also include new or enhanced features, or better compatibility with different devices or applications. They can also improve the stability of your software, and remove outdated features.



# 11. Financial Transactions

- **Any Financial Transaction should be verified by phone**
- **ACH and Wire Transfer Fraud is on the increase**
- **FBI reported 11,677 cases with \$221 million in losses**
- **Use 2 factor authentication on every transaction and double verify everything**

## 12. Website Security



- Hacked websites can target your customers
- The number of hacked sites rises rapidly
- Business reputation loss and drop in revenue
  - Website gets blacklisted



# Impress Computers Your Trusted IT Provider

At Impress Computers, we understand that as technology evolves, so do opportunities to evolve your business. In order to ensure your business evolves and thrives in today's world, we are always a few steps ahead, making security recommendations to fit your needs and mitigate the latest cyber threats. You can rest easy when you put your IT support needs in our hands.





# Q & A