Cybersecurity
Montenegro, 2019
Security Vs. Privacy

SunPlus
Technology, Distraction?

There were 500 apps on the first iteration of Apple’s App Store in 2008. In 2018, Apple announced that there were 20 million registered iOS developers. They have 500 million weekly visitors to the App Store alone. Total number of app downloads in 2018 was 194 billion.
The mission of the Seventh-day Adventist Church is to call all people to become disciples of Jesus Christ, to proclaim the everlasting gospel embraced by the three angels’ messages (Revelation 14:6-12), and to prepare the world for Christ’s soon return.
1 Corinthians 7:35 Now I say this for your own benefit—not to put a restraint on you, but to promote proper and constant service to the Lord without distraction.
Stay Focused
Stay Focussed

All your files have been encrypted!

All your files have been encrypted due to a software attack, and you must pay a ransom to decrypt them. Write this ID in the title of your message: 888btc888@keemail.me. In case of no answer in 24 hours, we will not be responsible for the lost data.

You have to pay for decryption in Bitcoins. The process may take up to 48 hours. You will receive a decryption tool that will decrypt all your files.

Free decryption as guarantee
Before paying you can send us up to 1 file for free decryption. The total size of files must be less than 1Mb (non archived), and files should not contain valuable information. (databases, backups, large excel sheets, etc.)

How to obtain Bitcoins
The easiest way to buy bitcoins is LocalBitcoins site. You have to register, click 'Buy bitcoins', and select the seller by payment method and price.
https://localbitcoins.com/buy_bitcoins
Also you can find other places to buy Bitcoins and beginners guide here:
http://www.coindesk.com/information/how-can-i-buy-bitcoins/
All your files have been encrypted!

All your files have been encrypted due to a security problem with your PC. If you want to restore them, write us to the e-mail 888btc888@keemail.me.

Write this ID in the title of your message: C6AF373F

In case of no answer in 24 hours write us to these e-mails: 888btc888@india.com

You have to pay for decryption in Bitcoins. The price depends on how fast you write to us. After payment we will send you the decryption tool that will decrypt all your files.

Free decryption as guarantee

Before paying you can send us up to 1 file for free decryption. The total size of files must be less than 1Mb (non archived), and files should not contain valuable information.

(databases, backups, large excel sheets, etc.)

How to obtain Bitcoins

The easiest way to buy bitcoins is LocalBitcoins site. You have to register, click ‘Buy bitcoins’, and select the seller by payment method and price.

https://localbitcoins.com/buy_bitcoins

Also you can find other places to buy Bitcoins and beginners guide here:

http://www.coindesk.com/information/how-can-i-buy-bitcoins/
Ooops, your files have been encrypted!

What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?
I sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>. But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don’t pay in 7 days, you won’t be able to recover your files forever. We will have free events for users who are so poor that they couldn’t pay in 6 months.

How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>. Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT from Monday to Friday.

Send $300 worth of bitcoin to this address:

Copy

Check Payment
Decrypt
Cyber Security Risks

1. DDoS
2. Hacking
3. Malware
4. Ransomware
5. Phishing (Most Often Used)
Ransomware

.- Today, we know that more than 1 out of every 5 businesses that are hit with Ransomware go out of business and cease all operations within a week or two after the attack occurs.

.- Ransomware impacts on-premise and cloud backups just the same.

.- The average cost to unlock the typical Ransomware attack has grown to around $10,000, the Ryuk strain of Ransomware now charges, on average, $288,000, per attack.

.- The latest studies show that Ransomware downtime costs each infected entity around $8,500 per hour of downtime.
The City of Johannesburg detected a network breach which resulted in unauthorised access to its information systems on Thursday afternoon by an unknown and unconfirmed group of hackers. As a precautionary measure, COJ has shut down several customer systems for about 24 hours.

The City of Johannesburg suffered a major network breach on Thursday 24 October 2019 when a group, reportedly known as the Shadow Kill Hackers, allegedly hacked into its system.

According to a report, the hackers left a bitcoin ransom note via Twitter. Business Day wrote that the hackers are demanding 4.0 bitcoins by 28 October at 5pm. If the City fails to do so they threatened to upload all the data they have procured onto the internet.

“All your servers and data have been hacked. We have dozens of back doors inside your city. We have control of everything in your city. We also compromised all passwords and sensitive data such as finance and personal population information,” the ransom note reportedly said.
City of Johannesburg Attack

Shadow Kill Hackers
DC TAKEOVER
### City of Johannesburg Attack

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Data</th>
<th>Timestamp</th>
</tr>
</thead>
<tbody>
<tr>
<td>(.same as parent folder)</td>
<td>Start of Authority (SOA)</td>
<td>[144.273.193]</td>
<td>static</td>
</tr>
<tr>
<td>(.same as parent folder)</td>
<td>Name Server (NS)</td>
<td>zayj03139wad04.johburg.local</td>
<td>static</td>
</tr>
<tr>
<td>(.same as parent folder)</td>
<td>Name Server (NS)</td>
<td>zayj03139wad04.johburg.local</td>
<td>static</td>
</tr>
<tr>
<td>(.same as parent folder)</td>
<td>Name Server (NS)</td>
<td>zayj03139wad04.johburg.local</td>
<td>static</td>
</tr>
<tr>
<td>(.same as parent folder)</td>
<td>Name Server (NS)</td>
<td>zayj03139wad04.johburg.local</td>
<td>static</td>
</tr>
<tr>
<td>(.same as parent folder)</td>
<td>Name Server (NS)</td>
<td>zayj03139wad04.johburg.local</td>
<td>static</td>
</tr>
<tr>
<td>(.same as parent folder)</td>
<td>Name Server (NS)</td>
<td>zayj03139wad04.johburg.local</td>
<td>static</td>
</tr>
<tr>
<td>(.same as parent folder)</td>
<td>Name Server (NS)</td>
<td>zayj03139wad04.johburg.local</td>
<td>static</td>
</tr>
<tr>
<td>(.same as parent folder)</td>
<td>Host (A)</td>
<td>168.89.180.19</td>
<td>static</td>
</tr>
<tr>
<td>(.same as parent folder)</td>
<td>Host (A)</td>
<td>168.89.175.14</td>
<td>static</td>
</tr>
<tr>
<td>(.same as parent folder)</td>
<td>Host (A)</td>
<td>168.89.250.12</td>
<td>static</td>
</tr>
<tr>
<td>(.same as parent folder)</td>
<td>Host (A)</td>
<td>168.89.115.27</td>
<td>static</td>
</tr>
<tr>
<td>(.same as parent folder)</td>
<td>Host (A)</td>
<td>168.89.121.204</td>
<td>static</td>
</tr>
<tr>
<td>(.same as parent folder)</td>
<td>Host (A)</td>
<td>168.89.250.237</td>
<td>static</td>
</tr>
<tr>
<td>(.same as parent folder)</td>
<td>Host (A)</td>
<td>168.89.180.7</td>
<td>static</td>
</tr>
<tr>
<td>(.same as parent folder)</td>
<td>Host (A)</td>
<td>168.89.121.203</td>
<td>static</td>
</tr>
<tr>
<td>(.same as parent folder)</td>
<td>Host (A)</td>
<td>168.89.181.11</td>
<td>static</td>
</tr>
<tr>
<td>(.same as parent folder)</td>
<td>Host (A)</td>
<td>168.89.232.5</td>
<td>static</td>
</tr>
<tr>
<td>(.same as parent folder)</td>
<td>Host (A)</td>
<td>168.89.101.10</td>
<td>static</td>
</tr>
<tr>
<td>(.same as parent folder)</td>
<td>Host (A)</td>
<td>168.89.7.27</td>
<td>static</td>
</tr>
<tr>
<td>(.same as parent folder)</td>
<td>404WWW</td>
<td>168.89.146.66</td>
<td>static</td>
</tr>
<tr>
<td>(.same as parent folder)</td>
<td>404WWW</td>
<td>168.89.150.4</td>
<td>static</td>
</tr>
<tr>
<td>(.same as parent folder)</td>
<td>404WWW</td>
<td>168.89.113.126</td>
<td>static</td>
</tr>
<tr>
<td>(.same as parent folder)</td>
<td>404WWW</td>
<td>168.89.74.119</td>
<td>static</td>
</tr>
<tr>
<td>(.same as parent folder)</td>
<td>404WWW</td>
<td>168.89.106.111</td>
<td>static</td>
</tr>
<tr>
<td>(.same as parent folder)</td>
<td>404WWW</td>
<td>168.89.145.39</td>
<td>static</td>
</tr>
<tr>
<td>(.same as parent folder)</td>
<td>404WWW</td>
<td>168.89.17.13</td>
<td>static</td>
</tr>
<tr>
<td>(.same as parent folder)</td>
<td>404WWW</td>
<td>168.89.40.4</td>
<td>static</td>
</tr>
<tr>
<td>(.same as parent folder)</td>
<td>404WWW</td>
<td>168.89.17.95</td>
<td>static</td>
</tr>
<tr>
<td>(.same as parent folder)</td>
<td>404WWW</td>
<td>168.89.51.175</td>
<td>static</td>
</tr>
<tr>
<td>(.same as parent folder)</td>
<td>404WWW</td>
<td>168.89.174.172</td>
<td>static</td>
</tr>
<tr>
<td>(.same as parent folder)</td>
<td>404WWW</td>
<td>168.89.80.129</td>
<td>static</td>
</tr>
<tr>
<td>(.same as parent folder)</td>
<td>404WWW</td>
<td>168.89.208.28</td>
<td>static</td>
</tr>
<tr>
<td>(.same as parent folder)</td>
<td>404WWW</td>
<td>168.89.72.33</td>
<td>static</td>
</tr>
<tr>
<td>(.same as parent folder)</td>
<td>404WWW</td>
<td>168.89.2.41</td>
<td>static</td>
</tr>
<tr>
<td>(.same as parent folder)</td>
<td>404WWW</td>
<td>168.89.10.35</td>
<td>static</td>
</tr>
<tr>
<td>(.same as parent folder)</td>
<td>404WWW</td>
<td>168.89.60.226</td>
<td>static</td>
</tr>
<tr>
<td>(.same as parent folder)</td>
<td>404WWW</td>
<td>168.89.61.80</td>
<td>static</td>
</tr>
<tr>
<td>(.same as parent folder)</td>
<td>404WWW</td>
<td>168.89.60.209</td>
<td>static</td>
</tr>
</tbody>
</table>
Ransomware Prevention
Best Practices

.- Do not pay the ransom.

.- Make sure you have Backups on premise and on cloud with a good retention policy

.- Use VPN

.- Do make sure that all systems and software are up-to-date with relevant patches.

.- Use Antivirus and Firewall and good security policies
All your files have been encrypted!

All your files have been encrypted due to a security problem with your PC. If you want to restore them, write us to the e-mail 888btc888@keemail.me. Write this ID in the title of your message C6AF373F.

In case of no answer in 24 hours write us to these e-mails: 888btc888@india.com

You have to pay for decryption in Bitcoins. The price depends on how fast you write to us. After payment we will send you the decryption tool that will decrypt all your files.

Free decryption as guarantee

Before paying you can send us up to 1 file for free decryption. The total size of files must be less than 1Mb (non archived), and files should not contain valuable information. (databases, backups, large excel sheets, etc.)

How to obtain Bitcoins

The easiest way to buy bitcoins is LocalBitcoins site. You have to register, click ‘Buy bitcoins’, and select the seller by payment method and price.

https://localbitcoins.com/buy_bitcoins

Also you can find other places to buy Bitcoins and beginners guide here:

http://www.coindesk.com/information/how-can-i-buy-bitcoins/
<table>
<thead>
<tr>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>E</th>
<th>F</th>
<th>G</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Name</td>
<td>ID(SUD\ldots)ID(SUD\ldots)</td>
<td>Password</td>
<td>IP</td>
<td>SUNPLUS</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Spicer</td>
<td>p@sswOrd</td>
<td>p@sswOrd</td>
<td>104.211.93.72</td>
<td>LHA</td>
<td></td>
</tr>
<tr>
<td></td>
<td>WIU</td>
<td>p@sswOrd</td>
<td>p@sswOrd</td>
<td>p@sswOrd</td>
<td>MMU</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SEIU</td>
<td>p@sswOrd</td>
<td>p@sswOrd</td>
<td>p@sswOrd</td>
<td>PGA</td>
<td></td>
</tr>
<tr>
<td></td>
<td>CMS</td>
<td>p@sswOrd</td>
<td>p@sswOrd</td>
<td>p@sswOrd</td>
<td>RAB</td>
<td></td>
</tr>
<tr>
<td></td>
<td>KCS</td>
<td>p@sswOrd</td>
<td>p@sswOrd</td>
<td>p@sswOrd</td>
<td>RCH</td>
<td></td>
</tr>
<tr>
<td></td>
<td>STC</td>
<td>p@sswOrd</td>
<td>p@sswOrd</td>
<td>p@sswOrd</td>
<td>SSW</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>p@sswOrd</td>
<td>p@sswOrd</td>
<td></td>
<td>SKA</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>p@sswOrd</td>
<td>p@sswOrd</td>
<td></td>
<td>IDM</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>p@sswOrd</td>
<td>p@sswOrd</td>
<td></td>
<td>MDJ</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>p@sswOrd</td>
<td>p@sswOrd</td>
<td></td>
<td>LPM</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>p@sswOrd</td>
<td>p@sswOrd</td>
<td></td>
<td>NJJ</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>p@sswOrd</td>
<td>p@sswOrd</td>
<td></td>
<td>VCS</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>p@sswOrd</td>
<td>p@sswOrd</td>
<td></td>
<td></td>
<td>STM</td>
</tr>
</tbody>
</table>
An account failed to log on.

Subject:
Security ID: NULL SID
Account Name: -
Account Domain: -
Logon ID: 0x0
<table>
<thead>
<tr>
<th>Security ID:</th>
<th>Account Name:</th>
<th>Account Domain:</th>
<th>Logon ID:</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSI\SLVUser2</td>
<td>SLVUser2</td>
<td></td>
<td>0x28F8570F</td>
</tr>
</tbody>
</table>

**Audit Success**

Logoff event details:

- Event ID: 4634
- Task Category: Logoff
- Date and Time: 11/09/2019 11:49:25 PM
- Keywords: Audit Success
- Source: Microsoft Windows security auditing.
- Event ID: 4634
- Task Category: Logoff
- Date and Time: 11/09/2019 11:49:25 PM
- Keywords: Audit Success
- Source: Microsoft Windows security auditing.
- Event ID: 4634
- Task Category: Logoff
- Date and Time: 11/09/2019 11:49:25 PM
- Keywords: Audit Success
- Source: Microsoft Windows security auditing.
- Event ID: 4634
- Task Category: Logoff
- Date and Time: 11/09/2019 11:49:25 PM
- Keywords: Audit Success
- Source: Microsoft Windows security auditing.
- Event ID: 4634
- Task Category: Logoff
- Date and Time: 11/09/2019 11:49:25 PM
- Keywords: Audit Success
- Source: Microsoft Windows security auditing.
- Event ID: 4634
- Task Category: Logoff
- Date and Time: 11/09/2019 11:49:25 PM
- Keywords: Audit Success
- Source: Microsoft Windows security auditing.
- Event ID: 4634
- Task Category: Logoff
- Date and Time: 11/09/2019 11:49:25 PM
- Keywords: Audit Success
- Source: Microsoft Windows security auditing.
- Event ID: 4634
- Task Category: Logoff
- Date and Time: 11/09/2019 11:49:25 PM
- Keywords: Audit Success
- Source: Microsoft Windows security auditing.
- Event ID: 4634
- Task Category: Logoff
- Date and Time: 11/09/2019 11:49:25 PM
- Keywords: Audit Success
- Source: Microsoft Windows security auditing.
- Event ID: 4634
- Task Category: Logoff
- Date and Time: 11/09/2019 11:49:25 PM
- Keywords: Audit Success
- Source: Microsoft Windows security auditing.
- Event ID: 4634
- Task Category: Logoff
- Date and Time: 11/09/2019 11:49:25 PM
- Keywords: Audit Success
- Source: Microsoft Windows security auditing.
- Event ID: 4634
- Task Category: Logoff
- Date and Time: 11/09/2019 11:49:25 PM
- Keywords: Audit Success
- Source: Microsoft Windows security auditing.
- Event ID: 4634
- Task Category: Logoff
- Date and Time: 11/09/2019 11:49:25 PM
- Keywords: Audit Success
- Source: Microsoft Windows security auditing.
- Event ID: 4634
- Task Category: Logoff
- Date and Time: 11/09/2019 11:49:25 PM
- Keywords: Audit Success
- Source: Microsoft Windows security auditing.
- Event ID: 4634
- Task Category: Logoff
- Date and Time: 11/09/2019 11:49:25 PM
- Keywords: Audit Success
- Source: Microsoft Windows security auditing.
Cybersecurity Best Practices

• Use VPN

• Understand your shared responsibility

• Compliance with identity and access restrictions

• Use secure endpoints

• Keep in mind that simple errors can cause massive damage
Cybersecurity Best Practices

• Keep in mind that simple errors can cause massive damage

Did you know that 91% of successful data breaches started with a spear phishing attack?
Your IT administrator has initiated a mandatory password reset for your organization due to a suspected hacking attempt.

Please create a new password immediately to ensure your account is protected.

CREATE NEW PASSWORD

© Microsoft Team. All rights reserved.
Due to a system error you were double charged for your last order. A refund process was initiated but could not be completed due to errors in your billing information.

REF CODE:2550CGE

You are required to provide us a valid billing address.

Click Here to Update Your Address

After your information has been validated you should get your refund within 3 business days.

We hope to see you again soon.

Amazon.com

Email ID: [Redacted]
Urgent: Mandatory Password Reset

IT <IT@sunplus.adventist.org>
GST Distribution Group
Wednesday, February 20, 2019 at 22:26
Show Details

Your IT administrator has initiated a mandatory password reset for your organization due to a suspected hacking attempt.

Please create a new password immediately to ensure your account is protected.

CREATE NEW PASSWORD

© Microsoft Team. All rights reserved.
Email Preview - Your friend tagged you in photos on Facebook

From: Facebook <notify@facebook.authentlcation.com>
Reply-to: Facebook <notify@facebook.authentlcation.com>
Subject: Your friend tagged you in photos on Facebook

This message was sent to itadmin@ted.adventist.org. If you don’t want to receive these emails from Facebook in the future, please unsubscribe.
Facebook,LLC. Attention: Department 415 P.O Box 90210 Columbus OH 90210
Status: Active

Started: 2 days, 12 hours, and 24 minutes ago.

<table>
<thead>
<tr>
<th></th>
<th>Clicked</th>
<th>Not Clicked</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Delivered</td>
<td>19</td>
<td>0</td>
</tr>
<tr>
<td>Total Clicked</td>
<td>5</td>
<td>0</td>
</tr>
<tr>
<td>Total Data Entered</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Click Percentage:

The percentage of users that are vulnerable to social media phishing attacks:

26.32%

Data-Entered Percentage:

The percentage of users that attempt to enter data on a spoofed login page:

0%
THE ROOT OF THE PROBLEM

“Who owns the information, he owns the world.”

Nathan Rothschild
1777-1836
The root of the problem

• **30%** of organizations have sensitive/confidential information leaked through email

• **28%** of phishing (email) attacks successfully steal your credentials

• **24%** of phishing attack successfully infects systems with malware

• **13%** of email as part of a CEO (Fraud) attack successfully trick one or more senior executive in the organization
Let’s talk Solution

• Antivirus: 60% of data breaches can be stopped with a good AV

• Multi-factor authentication.

• Defend against Ransomware attacks storing files in the cloud. Google drive for business or OneDrive for business.

• Educate employee on how to spot and report phishing emails, attachments, links and websites.

• Used corporate solutions cloud based is a way to be better protected.
Let’s talk Solution

<table>
<thead>
<tr>
<th>Retention Name</th>
<th>Days Online</th>
<th>Copies Online</th>
</tr>
</thead>
<tbody>
<tr>
<td>Daily</td>
<td>30</td>
<td>30</td>
</tr>
<tr>
<td>Weekly</td>
<td>31</td>
<td>5</td>
</tr>
<tr>
<td>Monthly</td>
<td>365</td>
<td>12</td>
</tr>
</tbody>
</table>