PJ Networks
Computer Services
Network Support ~ Security and Compliance ~ Managed Services

Quad
County
Business
Summit

CyberSecurity For YOUR Business

PJ Networks Computer Services

(434) 975-0122
info@pj-networks.com
www.pj-networks.com

What is…

WHAT IS CYBER-SAFETY?

Cyber-safety is a common term used to describe a set of practices, measures and/or actions you can take to protect personal information and your computer from attacks.

CYBER-SAFETY THREATS

First, let’ s talk about some common cyber-safety threats and the problems they can cause . . .

Viruses

Viruses infect computers through email attachments and file sharing. They delete files, attack other computers, and make your computer run slowly. One infected computer can cause problems for all computers on a network.

Hackers

Hackers are people who “trespass” into your computer from a remote location. They may use your computer to send spam or viruses, host a Web site, or do other activities that cause computer malfunctions.

Identity Thieves

People who obtain unauthorized access to your personal information, such as Social Security and financial account numbers. They then use this information to commit crimes such as fraud or theft.

Spyware

Spyware is software that “piggybacks” on programs you download, gathers information about your online habits, and transmits personal information. It may also cause a wide range of other computer malfunctions.

Best Practices

Best practices for **Public Wi-Fi Use**

Nothing of value…do not conduct online banking or make credit card purchases

Personal protection…make sure you have a good antivirus program and that your computer firewall is turned on

Stay secure…use all of the "best practices" for safe Internet browsing and e-mail usage

Personal VPN…such as ExpressVPN, NordVPN, CyberGhost, PrivateVPN, Avast SecureLine, PIA, …

Let's learn about **Securely Using Social Media**

Same rules apply for credentials:

Long and complex passwords need to continue to rule the day – ensure that your passwords are not easy or intuitive to crack

Only share what is necessary:

Especially true if sharing/using/promoting regarding your business

Remember the apps on your phone!

It's not just about minding your logins from your PC - these apps are on your phone!

Update/review frequently

Lessens the chance of you not noticing an issue with your online social media accounts

FaceBook just announced on 9/28/18 that 50 MILLION user accounts had potentially been compromised using stolen "View As" tokens

Online **Buying and Selling**

Buying

Look for the Lock

Most browsers will display a padlock in the address bar or the bottom status bar to indicate a secure session

Seek the "S"

"S" as in 'secure' tells you that your Connection is encrypted

Known and Trusted

Sites you know and trust are likely more secure by virtue of their reputation and proven track record

Selling

Credit Card Processing

If you accept credit card payments in your business you should only store numbers provided in a secure encrypted system. If you need to write down a number, ensure that the paper is shredded and disposed of after you have processed the transaction

Use Proven Tech

Get direction from your bank or credit card provider on any mobile credit card reader solutions

Encrypt Encrypt Encrypt

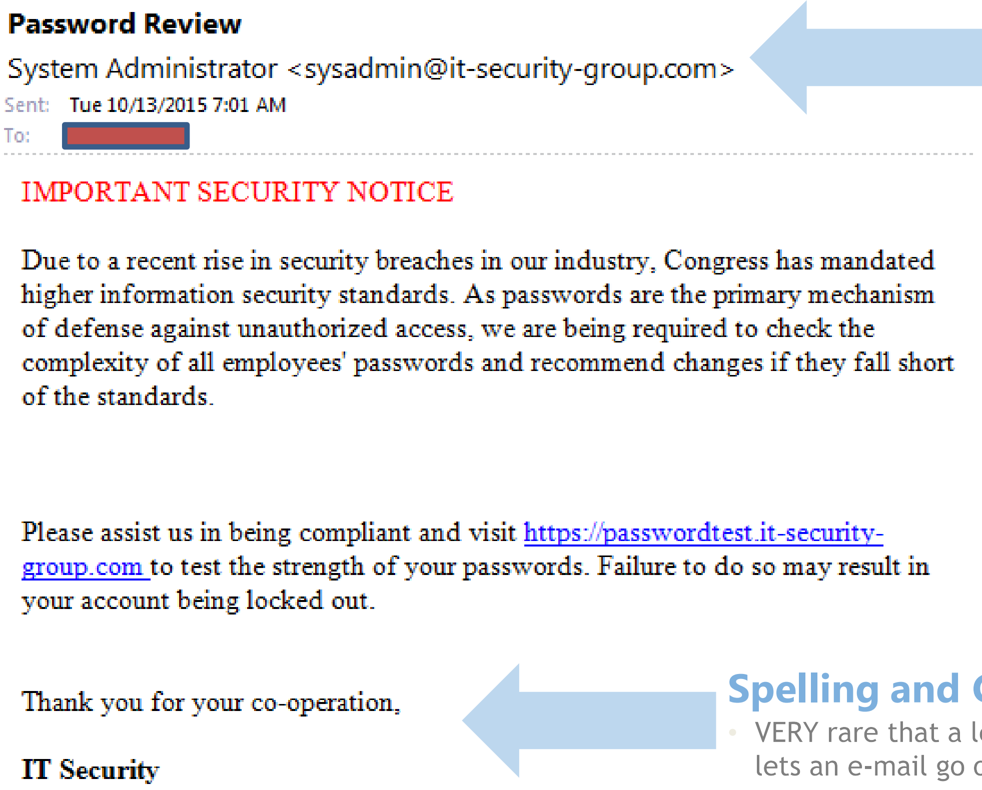
As the seller, it is YOUR responsibility to make sure that all transactions are conducted securely

I've actually called the company before I decided to do on-line business with them – and checked the BBB!

Scenario: **Phishing E-mail**

What are the "tells"?

REMEMBER! BE SUSPICIOUS!



Password Review

System Administrator <sysadmin@it-security-group.com>

Sent: Tue 10/13/2015 7:01 AM

To: [redacted]

IMPORTANT SECURITY NOTICE

Due to a recent rise in security breaches in our industry, Congress has mandated higher information security standards. As passwords are the primary mechanism of defense against unauthorized access, we are being required to check the complexity of all employees' passwords and recommend changes if they fall short of the standards.

Please assist us in being compliant and visit https://passwordtest.it-security-group.com to test the strength of your passwords. Failure to do so may result in your account being locked out.

Thank you for your co-operation,

IT Security

Subject and Sender

- Messages regarding passwords
- Generic e-mail addresses / unrecognizable addresses. EVEN if it looks legitimate, hover over it to see the actual address

Supposed Authority

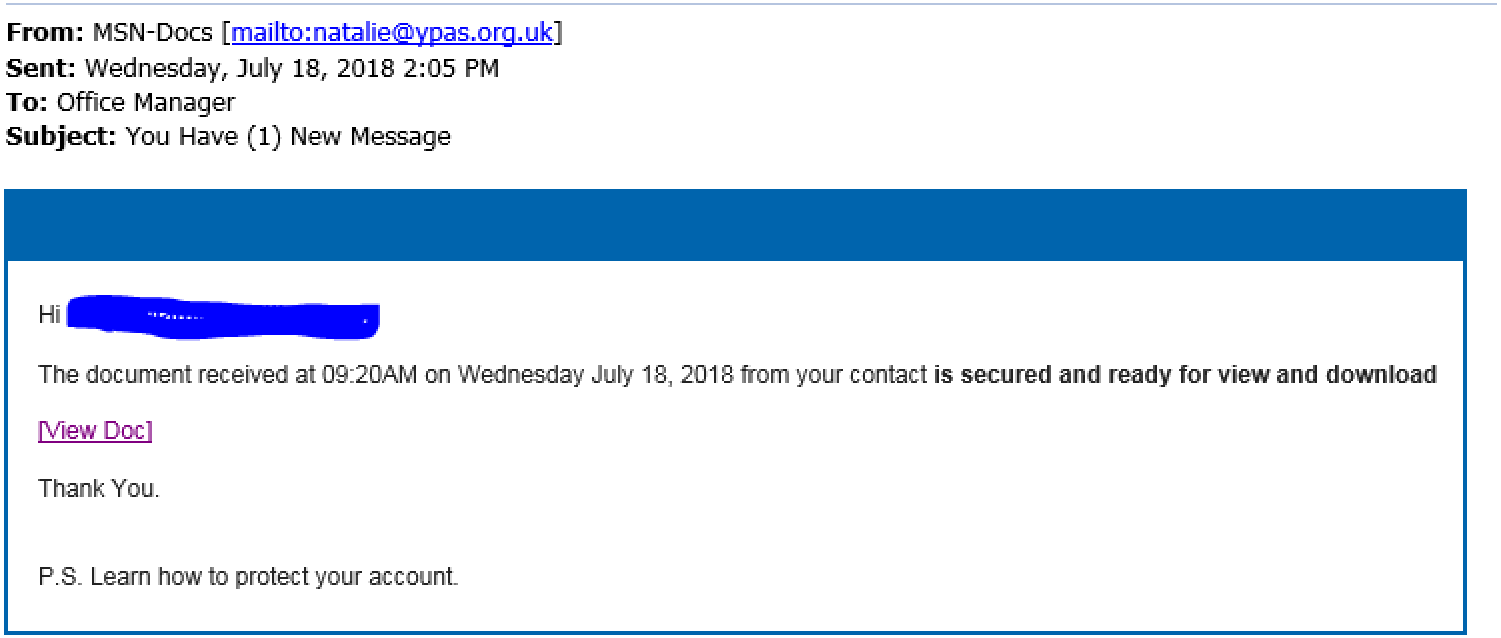
- Often cites some authority as the reason for the request

Asking for your password

- Most legitimate organizations will not ask
- Nothing legitimate will ask for multiple passwords

Spelling and Grammar

- VERY rare that a legitimate organization lets an e-mail go out with a misspelling



From: MSN-Docs [mailto:natalie@ypas.org.uk]
Sent: Wednesday, July 18, 2018 2:05 PM
To: Office Manager
Subject: You Have (1) New Message

Hi [redacted]

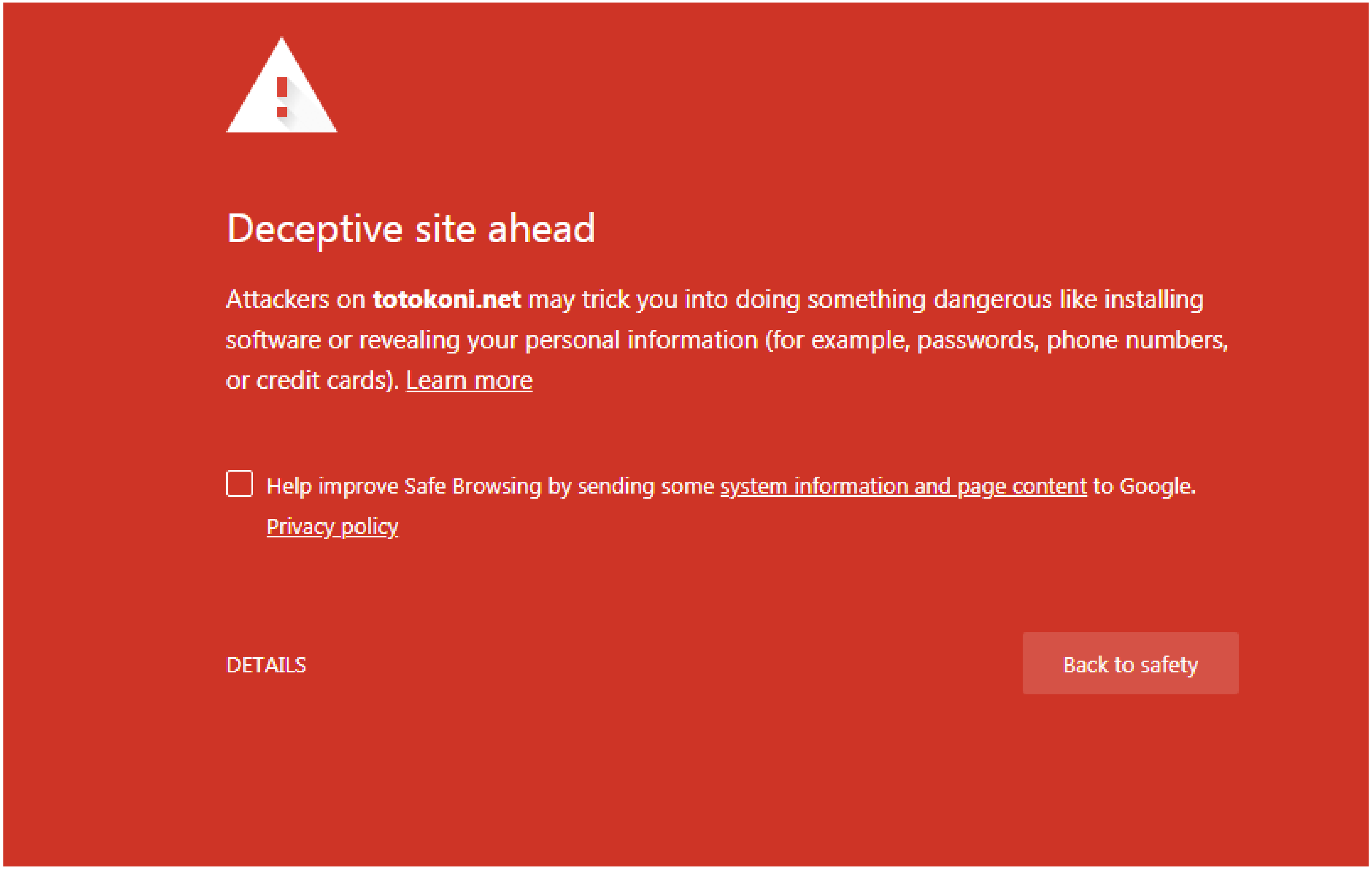
The document received at 09:20AM on Wednesday July 18, 2018 from your contact **is secured and ready for view and download**

[View Doc]

Thank You.

P.S. Learn how to protect your account.

https://totokoni.net/hbhgfvj/dgdgbee/index.php?email=office@REDACTED.com

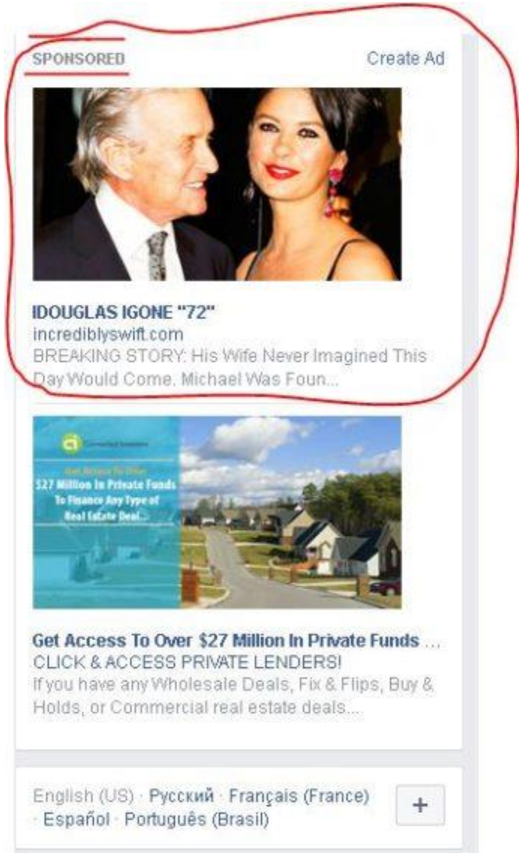


Deceptive site ahead

Attackers on **totokoni.net** may trick you into doing something dangerous like installing software or revealing your personal information (for example, passwords, phone numbers, or credit cards). Learn more

□ Help improve Safe Browsing by sending some system information and page content to Google. Privacy policy

Don’t Fall For Fake News or Fake Alerts!!

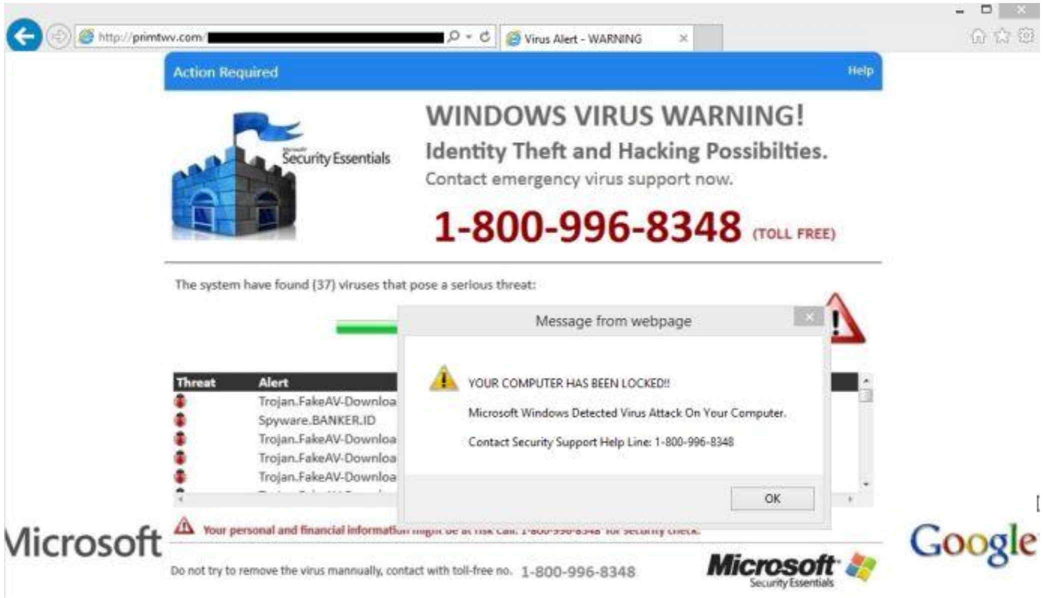


SPONSORED Create Ad

IDOUGLAS IGONE "72"
incrediblyswift.com
BREAKING STORY: His Wife Never Imagined This Day Would Come. Michael Was Foun...

Get Access To Over $27 Million In Private Funds ...
CLICK & ACCESS PRIVATE LENDERS!
If you have any Wholesale Deals, Fix & Flips, Buy & Holds, or Commercial real estate deals...

English (US) · Русский · Français (France) · Español · Português (Brasil)



http://primtwv.com/[redacted]

Virus Alert - WARNING

Action Required

WINDOWS VIRUS WARNING!
Identity Theft and Hacking Possibilties.
Contact emergency virus support now.
1-800-996-8348 (TOLL FREE)

The system have found (37) viruses that pose a serious threat:

Threat	Alert
	Trojan.FakeAV-Downloa
	Spyware.BANKER.ID
	Trojan.FakeAV-Downloa
	Trojan.FakeAV-Downloa
	Trojan.FakeAV-Downloa

Message from webpage

YOUR COMPUTER HAS BEEN LOCKED!!
Microsoft Windows Detected Virus Attack On Your Computer.
Contact Security Support Help Line: 1-800-996-8348

OK

Your personal and financial information might be at risk Call: 1-800-996-8348 for security check.

Do not try to remove the virus mannually, contact with toll-free no. 1-800-996-8348

Actions

Educate Yourself and Your Employees

You cannot assume that your employees know or understand even the most basic cybersecurity best practices, even though they may seem obvious to you.

PLEASE implement some kind of cybersecurity training program within your organization to discuss the ways that every member of your organization can help to protect your company from the many risks involved with the use of the Internet and modern technology solutions.

- You can find more about cyber-safety on the Cyber Security Library Web site (https://www.cybrary.it) and also find **free training** and tons of resources at https://smallbusinessbigthreat.com/virginia/

HOW PROTECTED IS YOUR SMALL BUSINESS?
Become a cybersecurity superhero for your business!

TOP SEVEN CYBER-SAFETY ACTIONS

Overview

1. Install OS/Software Updates

2. Run Anti-virus Software

3. Prevent Identity Theft

4. Turn on Personal Firewalls

5. Avoid Spyware/Adware

6. Protect Passwords

7. Back up Important Files

NOTE: Faculty and staff members should work with their technical support coordinator before implementing these measures.

Install OS/Software Updates

- Updates-sometimes called *patches*-fix problems with your operating system (OS) (e.g., Windows 7, Windows 10, Mac OS X) and software programs (e.g., Microsoft Office applications).
- Most new operating systems are set to download updates by default. After updates are downloaded, you will be asked to install them. Click **Yes**!
- Be sure to restart your computer after updates are installed so that the patches can be applied immediately.

Use Anti-Virus Software

- Periodically, check to see if your anti-virus is up to date by opening your anti-virus program and checking the *Last updated:* date.
- For business PC's, many Managed Service Providers (like PJ Networks) provide managed anti-virus solutions that are monitored and maintained remotely. Check with your technology solution provider.

*For a good, free anti-virus solution, use **Avast! Free Anti-Virus**, or **BitDefender Free**. Although the paid versions are better, these are generally a good alternative and better than no protection at all.*

Prevent Identity Theft

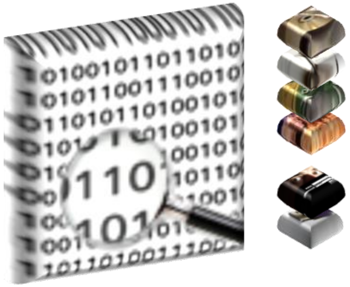
- Don't give out financial account numbers, Social Security numbers, driver's license numbers or other personal identity information unless you know exactly who's receiving it.
- Never send personal or confidential information via unencrypted e-mail or instant messages, as these can be easily intercepted.
- Beware of phishing scams - a quickly growing form of fraud that uses email messages that appear to be from a reputable business.
- Order a copy of your credit report from each of the three major credit bureaus- Equifax, Experian, and Trans Union.

Turn on Personal Firewalls

- Check your computer's security settings for a built-in personal firewall. If you have one, turn it on. Windows 7 & 10 and Mac OSX have built-in firewalls. For more information, see:
    - Mac Firewall (System Preferences→Security and Privacy)
        - (docs.info.apple.com/article.html?path=Mac/10.4/en/mh1042.html)
    - Microsoft Firewall (found in Control Panel)
        - (https://support.microsoft.com/en-us/help/4028544/windows-10-turn-windows-defender-firewall-on-or-off)

- Firewalls act as protective barriers between computers and the internet.

- Hackers search the Internet by sending out pings (calls) to random computers and wait for responses. Firewalls can prevent your computer from responding to these calls.



Avoid Spyware/Adware

- Spyware and adware take up memory and can slow down your computer or cause other problems.
- Watch for allusions to spyware and adware in user agreements before installing free software programs.
- Be wary of invitations to download software from unknown internet sources.
- PJ Networks Suggests using **Malwarebytes Free** or **Hitman Pro** for spyware and adware detection and removal.

Protect Passwords

- Do not share your passwords, and always make new passwords difficult to guess by avoiding dictionary words, and mixing letters, numbers and punctuation.

- Do not use one of these common passwords or any variation of them: qwerty1, abc123, letmein, password1, iloveyou1, (yourname1), baseball1.

- Change your passwords periodically.

- When choosing a password:
  - Mix upper and lower case letters
  - Use a minimum of 8 characters
  - Use mnemonics to help you remember a difficult password, or…
  - Use a long passphrase instead, like: **IWantToVisitDenverIn2018!**

- Store passwords in a safe place. Consider using LastPass, KeePass Password Safe (http://keepass.info/), Keychain (Mac) or an encrypted USB drive to store passwords. Avoid keeping passwords on a Post-it under your keyboard, on your monitor or in a drawer near your computer!

Back Up Important Files

- Reduce your risk of losing important files to a virus, computer crash, theft or disaster by creating back-up copies.
- Keep your critical files in one place on your computer's hard drive so they are regularly backed up, and use subfolders to separate data.
- Store your back-up media in a secure place away from your computer, in case of fire or theft.
- PJ Networks recommends testing file recovery from your backups on a monthly basis. Due to the risk of lost data, it is recommended in a business environment that all files are saved to a server for quick and easy recovery. Most businesses now use a cloud backup solution.

Additional Security Recommendations

- Use Two-Factor or Multi-Factor Authentication for online activity, such as Google Key, Google Authenticator or Duo's Unified Access Security

- Avoid leaving your laptop unsupervised and in plain view in the library or coffee house, in your car, or home.

- Set up a user account and password to prevent unauthorized access to your home computer files.

- Do not install unnecessary programs on your computer.

- Encrypt your local hard drive for extra security. (BitLocker, FileVault)

- Best practice dictates having your computer tuned up once every 6 months for home users. This keeps infectious software at bay and keeps the computer in top running condition.

CYBER-SAFETY AT WORK

- Be sure to work with network admins or IT support provider before implementing new cyber-safety measures.
- Review your Acceptable Use Policy to determine what is and isn’t allowed on your network in your company.
- Report to your supervisor any cyber-safety policy violations, security flaws/weaknesses you discover or any suspicious activity.
- Physically secure your computer by locking building/office doors and windows.
- Do not install unnecessary programs on your work computer.
  - Itunes, TorBrowsers, torrent applications, etc.

Cyber Services

CYBER-SAFETY SERVICES

Managed Service Providers (MSPs) offer services and software to help protect the network against cyber-safety attacks.

These include:

▪ Email Virus filtering ▪ Firewall services ▪ Email attachment filtering ▪ Vulnerability scanning ▪ Intrusion prevention ▪ Virus Cleanups	▪ Security Monitoring ▪ Managed Antivirus ▪ Cyber Security Training ▪ Network Policies ▪ Installation Assistance

For additional information about these and other cyber-safety services, please ask your technology solution provider

What should you **DO NEXT?**

1

Further Your Education

2

Assess Your Situation

3

Improve Your Situation

Your SBDC has invested in tools and resources to get you cyber-secure and ready for business!

http://smallbizbigthreat.com/virginia

PJ Networks

Computer Services

Network Support ~ Security and Compliance ~ Managed Services

FLUVANNA GREENE ORANGE LOUISA

Quad County Business Summit

CyberSecurity For YOUR Business

PJ Networks Computer Services

(434) 975-0122

info@pj-networks.com
www.pj-networks.com