PJ Networks
Computer Services

Network Support ~ Security and Compliance ~ Managed Services

Presents

CyberSecurity Basics

Protecting your Small Business Systems
In The Age of Artificial Intelligence

Prepared for the Members of the

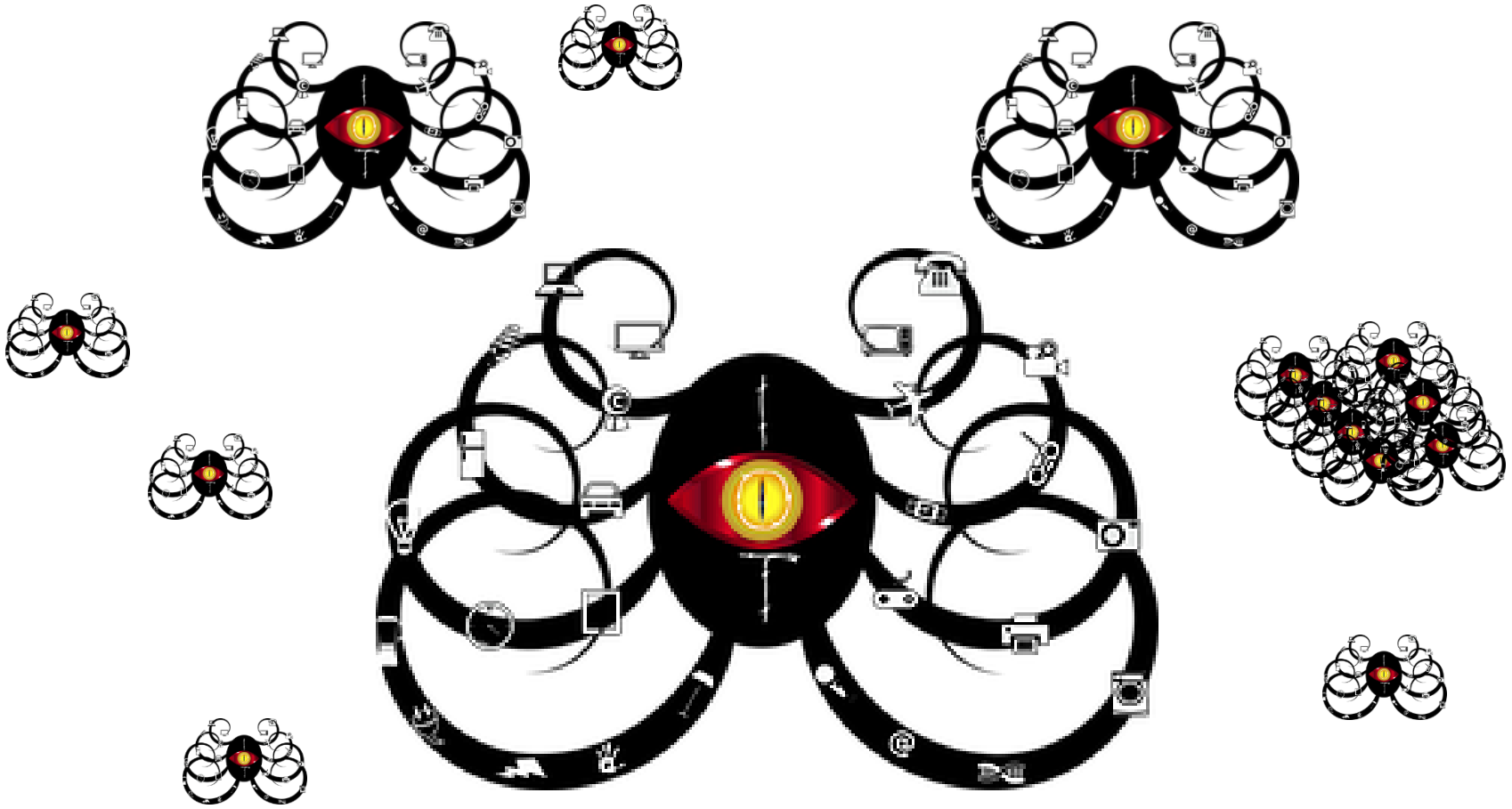
FLUVANNA CHAMBER

PJ Networks Computer Services
(434) 975-0122
info@pj-networks.com
www.pj-networks.com

PJ Networks
Computer Services

Network Support ~ Security and Compliance ~ Managed Services

Cybercriminals Are Touching
Everything, Everywhere, All The Time



AI Is Increasing Cyberthreats Exponentially

Threats

Traditional 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.

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

This is an example of REAL phishing spam sent to one of PJ Networks' clients and forwarded to us for review…

Note the sender's reply address

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**

This link → [View Doc]

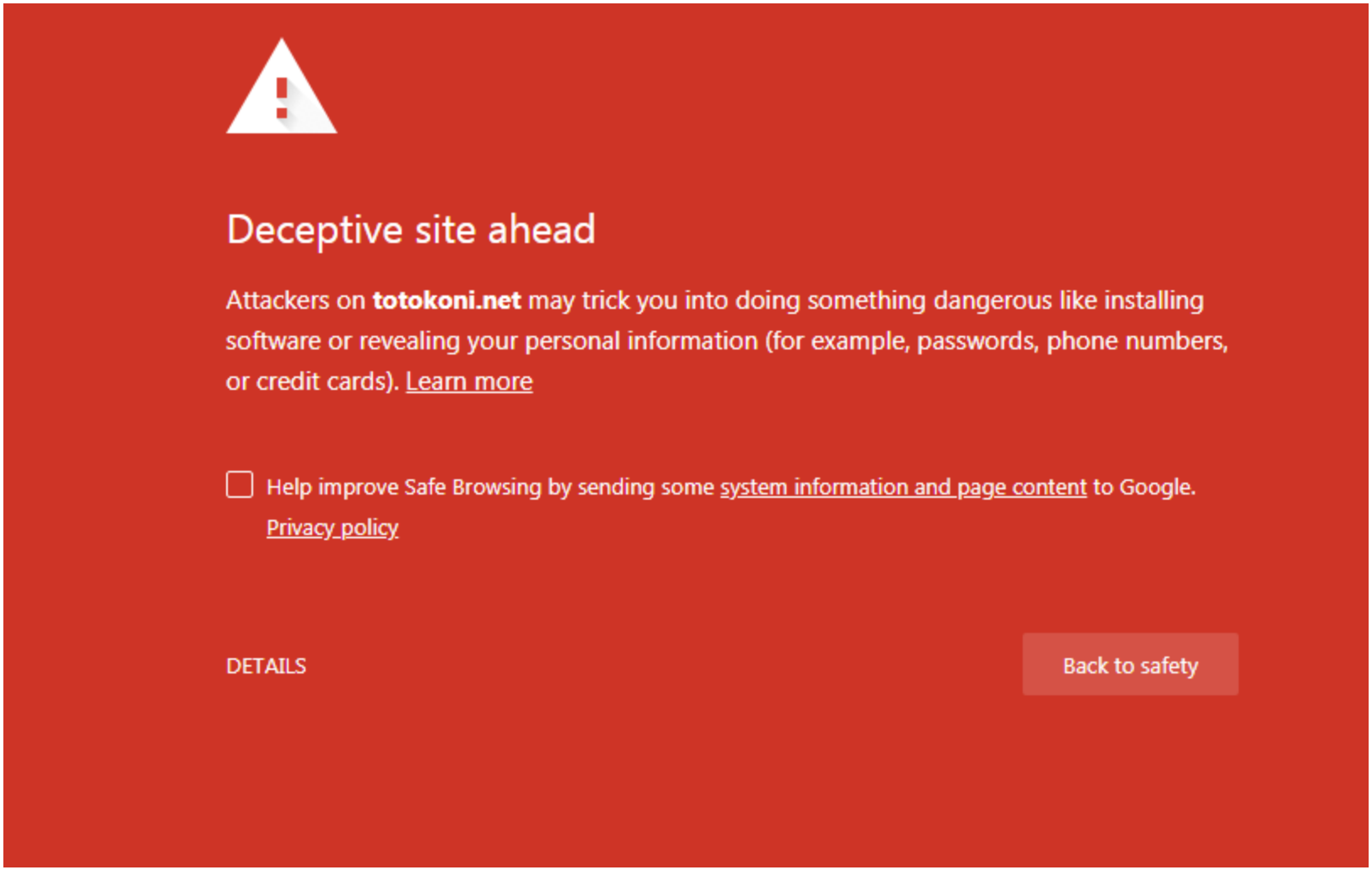
Thank You.

P.S. Learn how to protect your account.

Points to this website

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

…and this is what happened when the link was clicked on (by us)



Phishing and malware detection is **turned on** by default in Google Chrome
(we strongly recommend NOT turning it off!)

I entered this prompt into Microsoft's CoPilot AI to generate an e-mail to get users to click on a link:

My IT Support company manages hundreds of small businesses. We need to get all users to click on a link to change their Microsoft 365 password. Write an e-mail template that we can send out for that purpose.

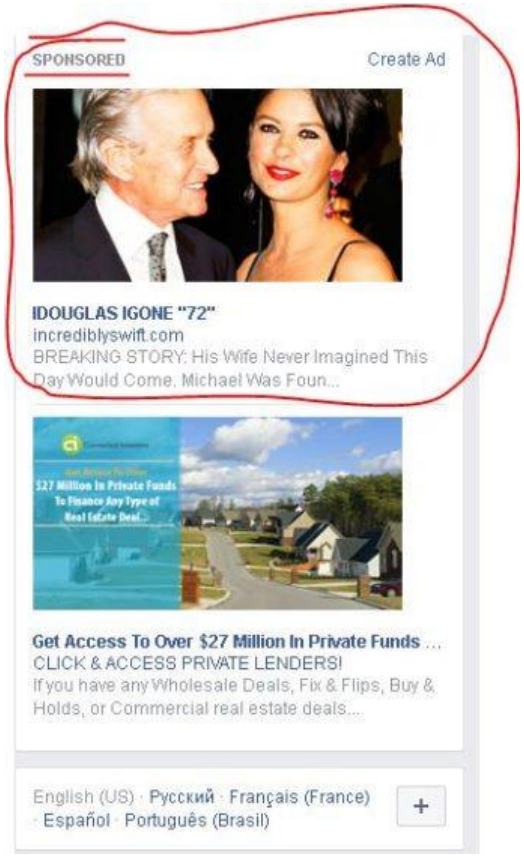
This is what it wrote for me:

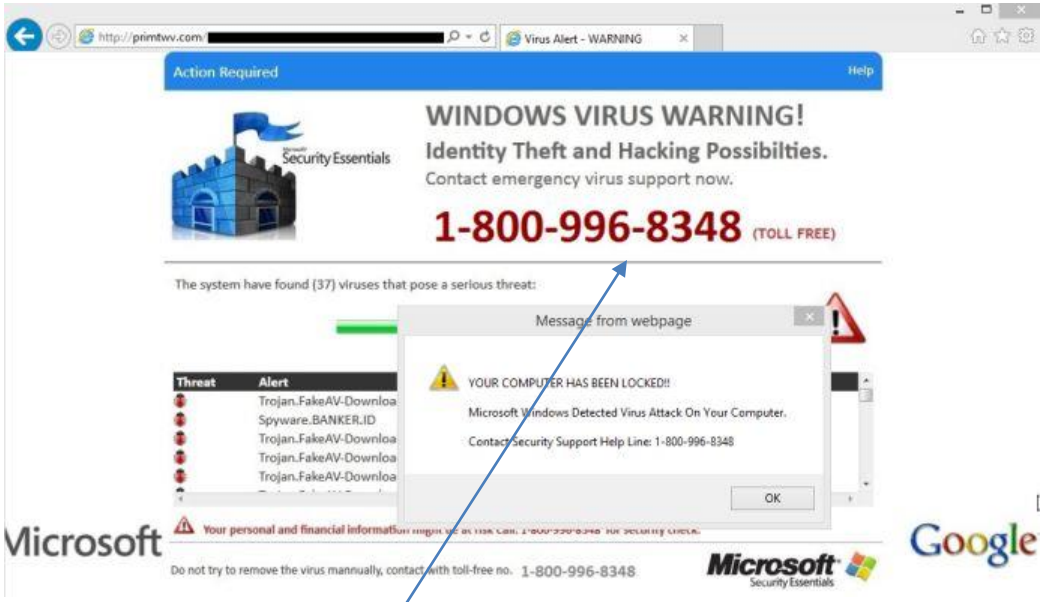
Here is a sample email template that you can use to request your users to change their Microsoft 365 password:

```
Subject: Action Required: Change Your Microsoft 365 Password

Dear [User],

We are writing to inform you that it is time to change your Microsoft 365 password. This is
a routine security measure that we take to ensure the safety of your account and data.

To change your password, please follow these steps:

1. Sign in to your Microsoft 365 account.
2. Click on your profile picture in the top right corner.
3. Select 'View account'.
4. Click 'Password'.
5. Follow the instructions to change your password.

Please note that your new password must meet the following requirements:

- At least 8 characters long
- Contains at least one uppercase letter
- Contains at least one lowercase letter
- Contains at least one number or symbol

If you have any questions or concerns, please do not hesitate to contact us.

Thank you for your cooperation.

Best regards,
[Your IT Support Company]
```

I hope this helps!

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





THIS CAN DRAIN YOUR BANK ACCOUNT!!!

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

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 10, Windows 11, Mac OS) and software programs (e.g., Microsoft Office, Adobe, Java 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 Endpoint Protection Software

- Periodically, check to see if your antivirus or EDR 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 endpoint solutions that are monitored and maintained remotely. Check with your technology solution provider.

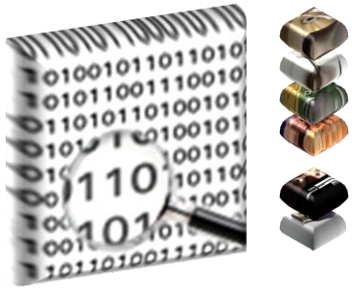
*For a good, free anti-virus solution, use **Windows Defender**, **Avast! Free Anti-Virus**, or **BitDefender Free**. Although the paid versions are better, these are generally a good alternative and better than no protection at all.* **PJ Networks recommends SentinelOne.**

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. That is how Social Engineering is used to steal your personal information!
- **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.
- **Use MFA for all your online accounts.**

Turn on Personal Firewalls

- Check your computer's security settings for a **built-in personal firewall**. If you have one, turn it on. Windows 10 & 11 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 **noticeable problems**.
- **Watch for allusions to unwanted programs (spyware and adware) in user agreements before installing free software programs.**
- Be wary of invitations to download software from unknown vendors or Internet sources. (especially free software)
- PJ Networks Suggests running **Malwarebytes Free** monthly for supplemental spyware and adware detection and removal.

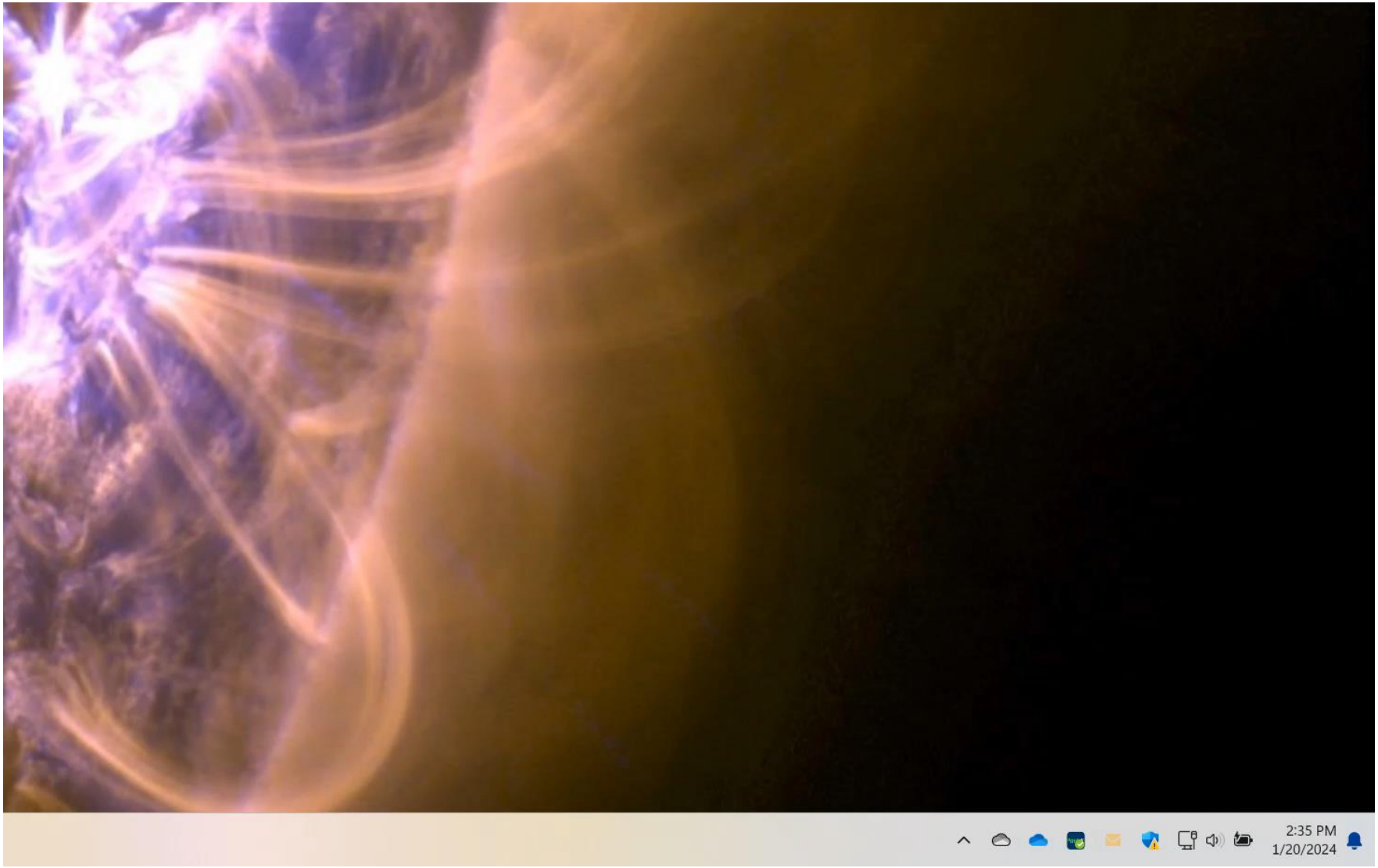
PROTECT PASSWORDS

- **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 BitWarden, 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!

- Reduces 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.
- Microsoft Windows 11 allows you to backup your personal data to OneDrive – please use it!

Microsoft Windows 11 allows you to backup your personal data to OneDrive



It’s that easy! ☺

Additional Security Recommendations

- **Use Two-Factor or Multi-Factor Authentication (MFA)** 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 **even at 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. (especially free ones)
- **Encrypt your local hard drive** for extra security. (BitLocker, FileVault)
- Best practice dictates **having your computer cleaned and tuned up annually**. This keeps infectious software at bay and keeps the computer in top running condition.
- **DO NOT use same password on multiple sites!!** (Password sprays)
- **Use a password manager** such as BitWarden or 1Password

Tips for Mac users

Macs used to only account for around 3% of infected computers, but have risen to a much higher percentage: 15% - 18%. Hackers have realized that in general, Mac users feel less vulnerable to security risks, and therefore are generally easier to catch with their guard down.

Here are a few recommendations for Mac users to protect their computer systems:

- **Use a third-party antivirus software** in conjunction with the built-in protection
  - Avast Security for Mac: https://www.avast.com/en-us/free-mac-security (Free or Premium)
  - Malwarebytes for Mac: https://www.malwarebytes.com/mac/
- There are a growing number of ransomware infections written **specifically to target Apple computers**: https://cointelegraph.com/news/mac-users-beware-new-ransomware-targets-apple-computers
- Most of the guidelines that apply to Windows users also apply to Mac users
- Here is a website with some more Mac-oriented security tips:
  - https://us.norton.com/internetsecurity-privacy-mac-security-tips-and-settings.html

NOTE: PJ Networks' computer repair shop are very experienced working on **older** Apple systems!


MOST small businesses are not prepared...
ISLAND OF MISFIT TOYS

For this

CYBERSECURITY SERVICES

Managed Service Providers (MSPs) offer services and software to help protect business networks against cyber-safety attacks that most small businesses cannot manage or afford on their own.

▪ Email Virus filtering	▪ Realtime Security Monitoring
▪ Firewall services	▪ Managed Endpoint Protection
▪ Remote VPN with MFA	▪ Cyber Security Training
▪ Email attachment filtering	▪ Phishing Simulations
▪ Vulnerability scanning	▪ Dark Web Monitoring
▪ Intrusion prevention	▪ Network Security Policies
▪ Cloud Backups	▪ Installation Assistance
▪ Priveleged Access Management (PAM)	▪ Cloud Backups
▪ Microsoft 365 Tenant Monitoring	▪ Microsoft and Google Backups

Hacking as a Service: How This New Offering Is Changing the Threat Landscape

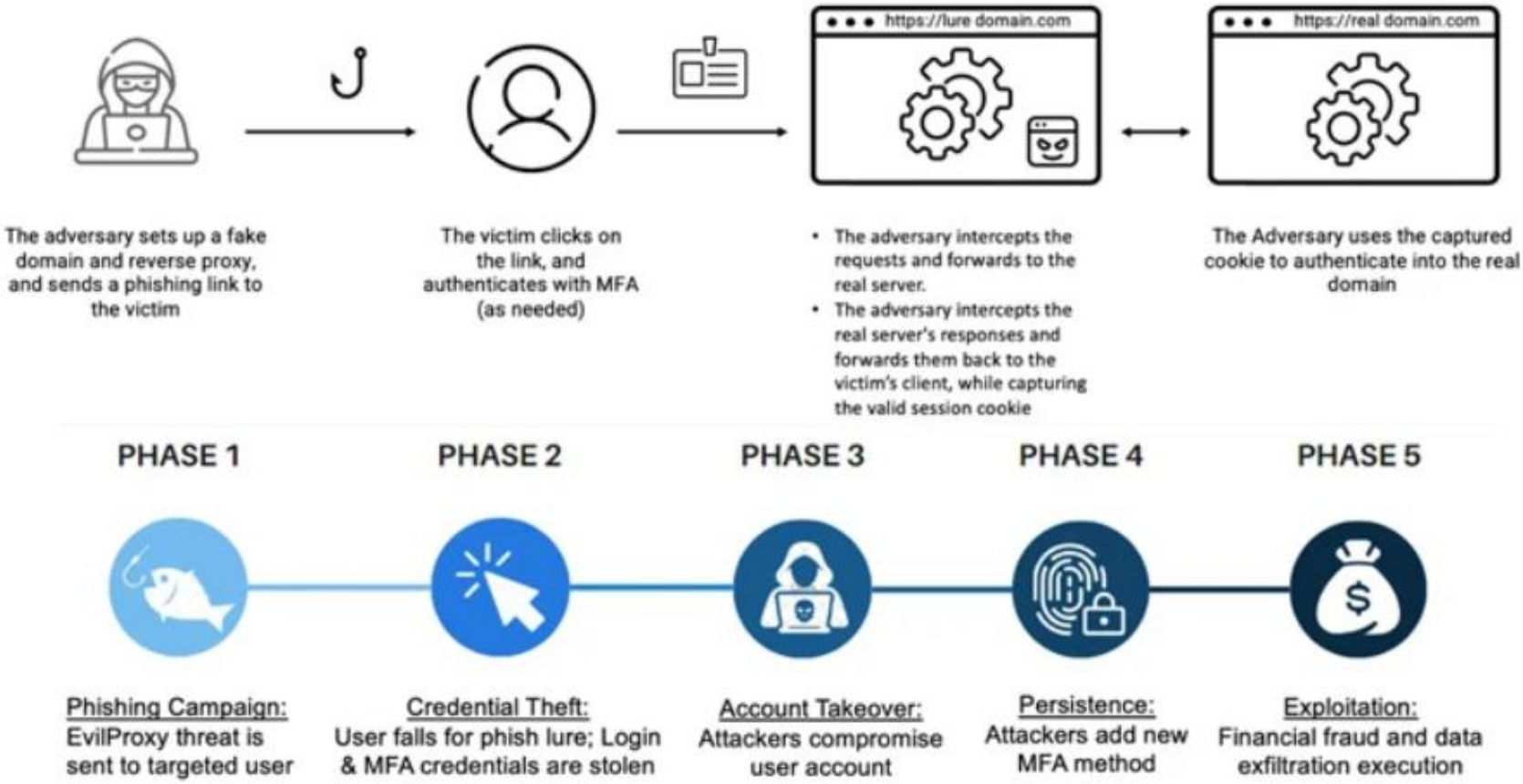
Pulling off a successful phishing attack used to require a skilled blend of technical knowledge and social engineering to create a legitimate looking campaign. Today, much of the hard work can be bought online, bundled into "phishing kits," which are software packages that streamline the process of copying a site design and uploading it to a web server as a phishing site.

A phishing kit may include:

1. Fake Domain: preferably deceptively similar to a known legitimate site
2. Fake Login Page: preferably one that resembles the original
3. SMTP Server: one of several methods to send a large amount of spam anonymously
4. Bulk Mailer Software
5. Leads: lists of target email addresses

- Phishing kits don't just enable hackers to run their own phishing campaign, but enable them to run them quickly in an effort to avoid detection. In the past, phishing websites might be live for days to weeks, today they can be live for only a few hours.

Cybercriminals Increasingly Using EvilProxy Phishing Kit to Target Executives



Hackers are selling the data of millions lifted from 23andMe's genetic database

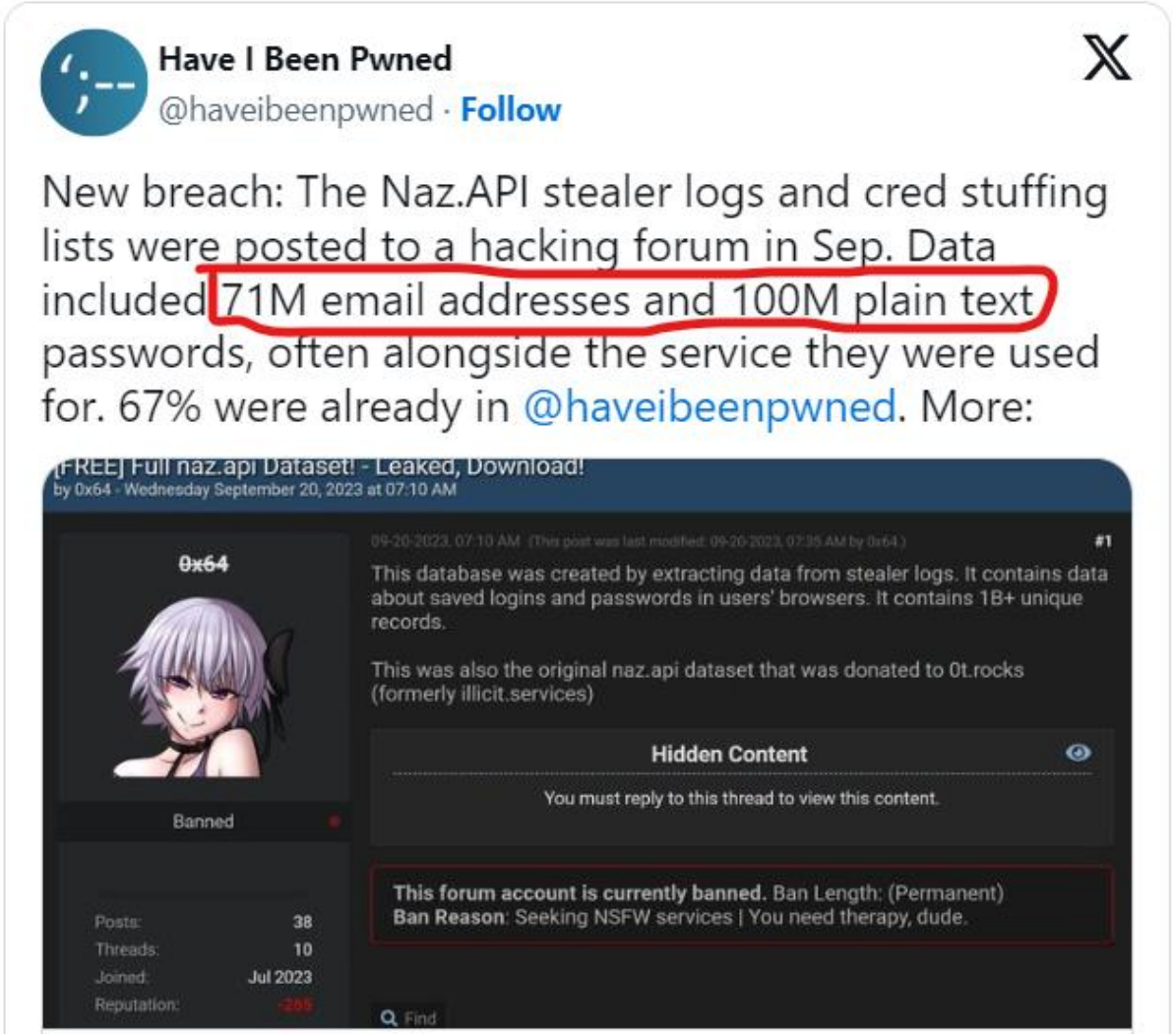
followed by…

Hacker trying to sell data of people with Jewish ancestry taken from genetic testing company

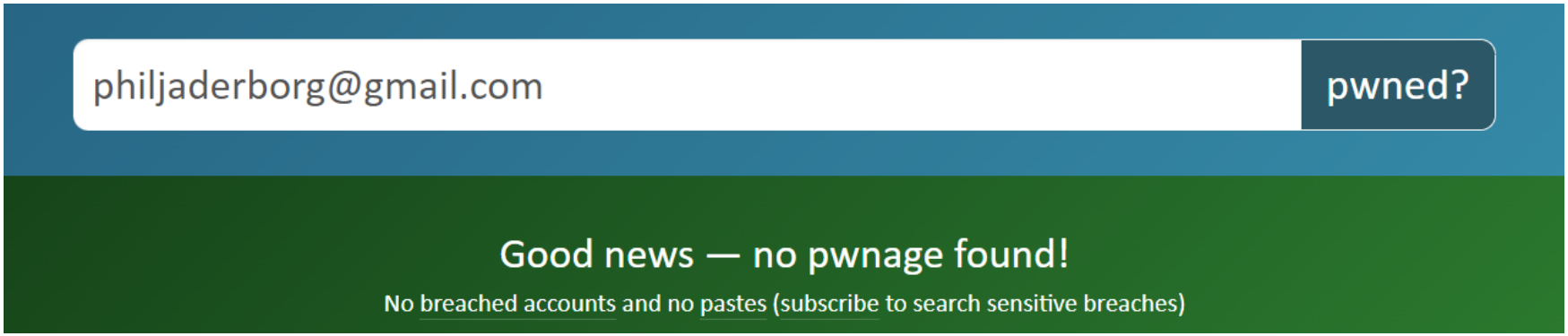
Ransomware Actor Uses TeamViewer to Gain Initial Access to Networks: Attackers have increasingly leveraged the widely used remote access tool, installed on hundreds of millions of endpoints, to break into victim environments.

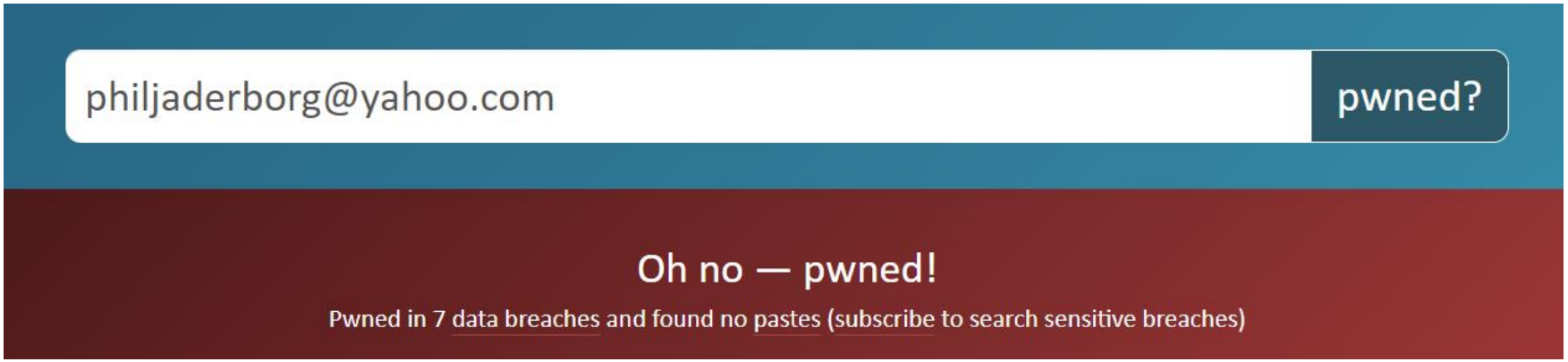
Quantum computing to spark 'cybersecurity Armageddon,' IBM says: Governments and businesses are not prepared for the havoc quantum computers will sow in cybersecurity by the end of the decade, according to an International Business Machines Corp. executive.

MASSIVE RELEASE OF BREACHED PASSWORDS LIKELY INCLUDES YOURS

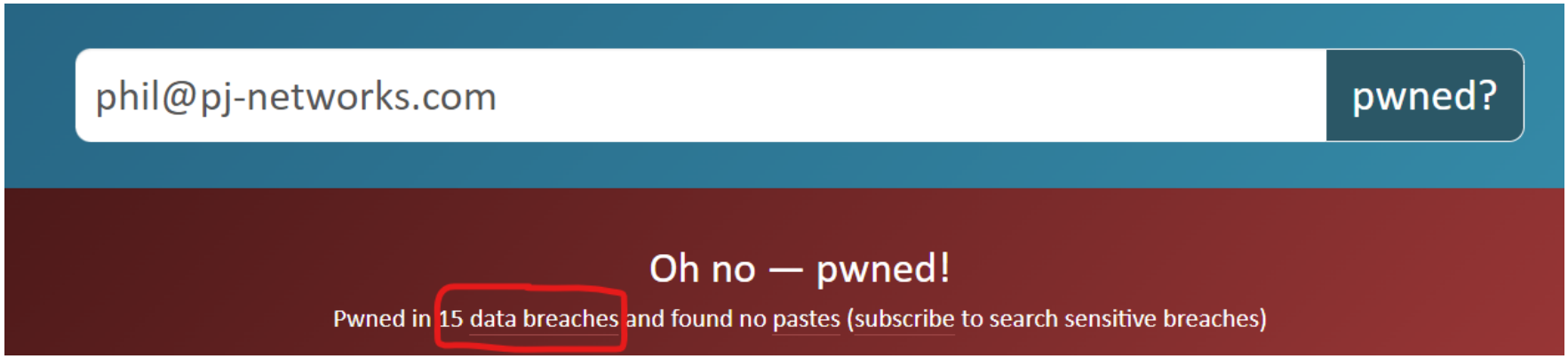


Go To https://haveibeenpwned.com to check your e-mail address



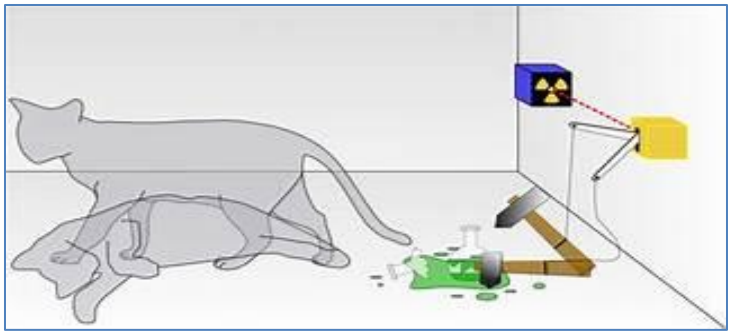


…and the big one:



Quantum Computing and Schrodinger's Cat

Schrödinger's cat is a thought experiment in quantum mechanics that illustrates a paradox of quantum superposition. In the experiment, a hypothetical cat is placed in a sealed box with a flask of poison and a radioactive source connected to a Geiger counter. If the counter detects radioactivity, the flask is shattered, releasing the poison and killing the cat. The Copenhagen interpretation of quantum mechanics implies that, after a while, the cat is **simultaneously alive and dead**. However, when one looks in the box, one sees the cat either alive or dead, not both alive and dead.



A **bit** is the smallest unit of digital information that can be processed by a computer. It can have one of two values: 0 or 1. In binary notation, 0 represents the absence of an electrical signal, while 1 represents the presence of an electrical signal.

0 or 1 = 1 bit

A **byte** is a unit of digital information that most commonly consists of eight bits. Unlike a bit, which can only represent one of two states, a byte can represent **256** (2^8) states.

01010101
00001111 = bytes of data
11111111

Now, let’s talk about

Quantum Entanglement…..

{ just kidding }

QUANTUM COMPUTING

Quantum computing is a technology that uses the principles of quantum physics to perform computations that are too complex or time-consuming for classical computers. Quantum computers use **quantum bits**, or qubits, which can exist in superpositions of two states, such as 0 and 1. This allows quantum computers to explore multiple possibilities simultaneously and solve problems faster or more efficiently than classical computers.

Breaking encryption: Quantum computers can potentially break the encryption methods that protect the security and privacy of online transactions, communications, and data. This could expose sensitive information, compromise digital identities, and enable cyberattacks[1][2][3].

Creating new threats: Quantum computers can also create new types of threats that are not possible with classical computers, such as **quantum hacking**, **quantum malware**, or **quantum sabotage**. These could affect the integrity, availability, and reliability of quantum systems and networks.

Outpacing regulations: Quantum computing is developing rapidly, but the regulations and standards that govern its use and impact are lagging behind. This could create ethical, legal, and social challenges, such as ensuring accountability, fairness, and transparency of quantum applications.

Enhancing artificial intelligence: Quantum computing can also enhance the capabilities and performance of artificial intelligence, such as machine learning, natural language processing, or computer vision. This could lead to breakthroughs in science, medicine, or engineering, but it could also raise ethical and social issues, such as the loss of human control, the misuse of data, or the bias and discrimination of algorithms .

How Much Faster ***is*** Quantum Computing?

Quantum's potential speedup:

Exponential advantage: For specific problems like factoring large numbers (used in encryption), quantum algorithms like Shor's can be **millions or even billions of times faster than classical algorithms**. In 2019, Google's Sycamore achieved "quantum supremacy" by solving a specific problem in 200 seconds that would take the world's fastest supercomputer 10,000 years.

Superposition and entanglement: These unique quantum properties allow simultaneous exploration of multiple possibilities, potentially speeding up optimization problems like chemical simulations or logistics planning.

So what ***can*** you do
to protect your business…?

Cyber Insurance is a Good Start!

But, remember: You have to answer the questions accurately and honestly. Otherwise, your policy will be worthless and your claims will be denied.

Example: Your insurance questionnaire asks “Are you enforcing MultiFactor Authentication (MFA) on all of your online business accounts?”.

You answer “Yes”, even though MFA is not turned on for your Microsoft 365 accounts or mailboxes. Hackers get into your Microsoft tenant, intercept an invoice for $20,000 and substitute their own routing and account numbers, then send it along to you for payment. You pay the invoice, then realize that it was a scam. You file a claim for the lost amount.

Will your cyber insurance company honor your claim and cover the lost $20,000? Probably not. (And rightfully so)

Hire a *proactive* Managed Service Provider (MSP) like PJ Networks

1	**Business-class VPN Firewall with Advanced Threat Protection**	• Perimeter protection—the first line of defense • Inspects all inbound and outbound traffic for malicious content • Blocks access to malicious websites • Provides secure VPN connections with MFA capability
2	**Realtime Computer and Network Monitoring with Alerts**	• Computer health checks are run daily (hard drive, CPU, memory, etc.) • Server checks are run hourly hard drive, CPU, memory, etc.) • Monitors security settings (firewall, UAC, resource spikes, etc.) • Provides remote support access and management
3	**Advanced Endpoint Detection And Response (EDR)**	• A unique, next-gen cybersecurity platform • Prevents, detects, responds, and hunts throughout all enterprise assets • Powered by Artificial Intelligence assistance • A real time autonomous network-wide security layer
4	**Privileged Access Management**	• PAM is based on the principle of least privilege needed • No employee has admin rights on local systems or network • Elevation control is managed through automated prompts • Approved tasks are automatically elevated with admin rights
5	**Microsoft 365 Tenant Monitoring**	• Monitors for suspicious activity • Verifies that MFA is enabled for user accounts • Provides security configuration reports • Realtime alerts for aggressive suspicious events
6	**E-mail Spam and Virus Filter With Advanced Phishing Protection**	• Two antivirus engines scan for malicious content • Attachment checking with Sandboxing • URL rewrites for Internet links • End user controls quarantine settings
7	**Microsoft and Google Workspace Full Cloud Backups**	• Daily backups of entire online user accounts • Microsoft 365: Mailbox, Calendar, Contacts, OneDrive Teams, Sharepoint • Google Workspace: Gmail, Chat, Meet, Calendar, Maps, Drive for storage • 10-year retention, fully indexed and searchable
8	**CyberLookout™ Sentry Protection**	• Dark Web Scans for Client Data Compromises • Weekly 3-minute employee Vulnerability Awareness Training • Short quizzes to test employee comprehension and retention • Random bi-monthly e-mail phishing simulations
9	**Full Server Image Cloud Backups with Local Cache**	• One full image backup to begin the cloud replication • Incremental backups every four hours to prevent significant data loss • Local hard drive with a local copy to expedite full system recovery process • Backups can be virtualized in the cloud for Emergency Disaster Scenarios
**	**ELEVATED SECURITY FOR COMPLIANCE: SOC/SIEM**	• **Satisfies many advanced PCI, HIPAA, NIST and CMMC requirements** • Advanced threat detection and response management solution • Monitors Microsoft 365 tenants in-depth for many types of threats • Flexible log retention to accommodate specific compliance needs

What Security Components Are Included In Our Support Plans?

PJ Networks
Multilayered Approach To Cybersecurity

Professional Edge

Executive and Corporate Edge

ALL BUSINESSES WITH SERVERS NEED THIS!

1	**Business-class VPN Firewall with Advanced Threat Protection**	♦ Perimeter protection—the first line of defense ♦ Inspects all inbound and outbound traffic for malicious content ♦ Blocks access to malicious websites ♦ Provides secure VPN connections with MFA capability
2	**Realtime Computer and Network Monitoring with Alerts**	♦ Computer health checks are run daily (hard drive, CPU, memory, etc.) ♦ Server checks are run hourly hard drive, CPU, memory, etc.) ♦ Monitors security settings (firewall, UAC, resource spikes, etc.) ♦ Provides remote support access and management
3	**Advanced Endpoint Detection And Response (EDR)**	♦ A unique, next-gen cybersecurity platform ♦ Prevents, detects, responds, and hunts throughout all enterprise assets ♦ Powered by Artificial Intelligence assistance ♦ A real time autonomous network-wide security layer
4	**Privileged Access Management**	♦ PAM is based on the principle of least privilege needed ♦ No employee has admin rights on local systems or network ♦ Elevation control is managed through automated prompts ♦ Approved tasks are automatically elevated with admin rights
5	**Microsoft 365 Tenant Monitoring**	♦ Monitors for suspicious activity ♦ Verifies that MFA is enabled for user accounts ♦ Provides security configuration reports ♦ Realtime alerts for aggressive suspicious events
6	**E-mail Spam and Virus Filter With Advanced Phishing Protection**	♦ Two antivirus engines scan for malicious content ♦ Attachment checking with Sandboxing ♦ URL rewrites for Internet links ♦ End user controls quarantine settings
7	**Microsoft and Google Workspace Full Cloud Backups**	♦ Daily backups of entire online user accounts ♦ Microsoft 365: Mailbox, Calendar, Contacts, OneDrive Teams, Sharepoint ♦ Google Workspace: Gmail, Chat, Meet, Calendar, Maps, Drive for storage ♦ 10-year retention, fully indexed and searchable
8	**CyberLookout™ Sentry Protection**	♦ Dark Web Scans for Client Data Compromises ♦ Weekly 3-minute employee Vulnerability Awareness Training ♦ Short quizzes to test employee comprehension and retention ♦ Random bi-monthly e-mail phishing simulations
9	**Full Server Image Cloud Backups with Local Cache**	♦ One full image backup to begin the cloud replication ♦ Incremental backups every four hours to prevent significant data loss ♦ Local hard drive with a local copy to expedite full system recovery process ♦ Backups can be virtualized in the cloud for Emergency Disaster Scenarios
**	**ELEVATED SECURITY FOR COMPLIANCE: SOC/SIEM**	♦ **Satisfies many advanced PCI, HIPAA, NIST and CMMC requirements** ♦ Advanced threat detection and response management solution ♦ Monitors Microsoft 365 tenants in-depth for many types of threats ♦ Flexible log retention to accommodate specific compliance needs

Professional Edge = You pay for additional service and support

Executive Edge = Includes UNLIMITED Remote Service and Support

Corporate Edge = UNLIMITED Remote and On Site Service and Support

PJ Networks Computer Services
(434) 975-0122 www.pj-networks.com
520 Greenfield Terrace Charlottesville, VA 22901

What should you **DO NEXT?**

- You can find more about cyber-safety on the Virginia SBDC website (https://www.virginiasbdc.org/programs/cybersecurity/) and also find **free training** and tons of resources at
- https://michigansbdc.org/small-business-big-threat-home/

PJ Networks

Multilayered Approach To Cybersecurity

FLUVANNA CHAMBER

CyberSecurity For Your Protection

PJ Networks Computer Services

(434) 975-0122

info@pj-networks.com

www.pj-networks.com