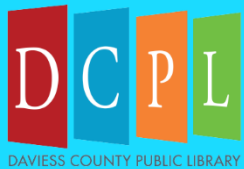


AVOIDING RANSOMWARE

Cheap Solutions to Protect Your Network



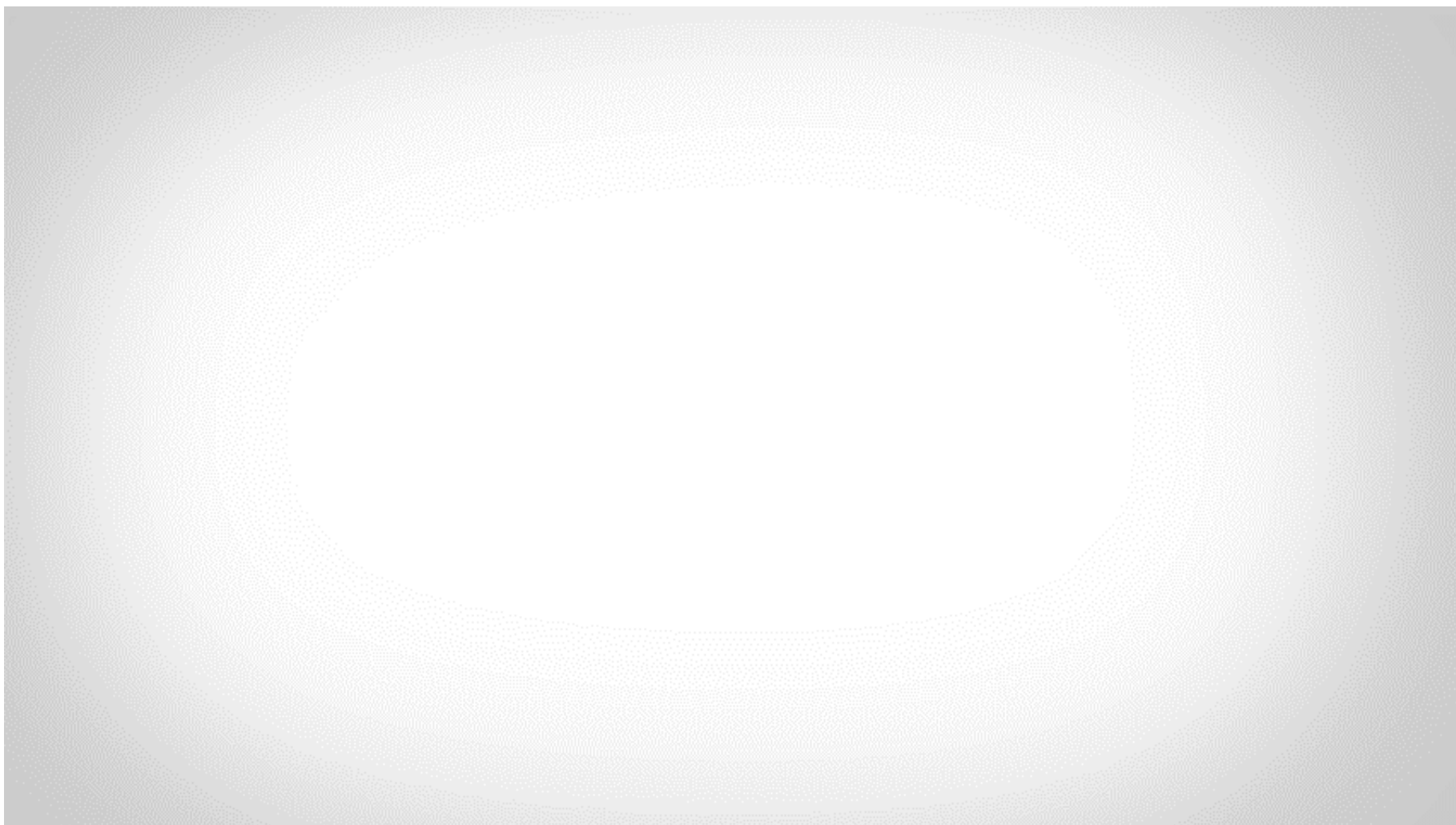
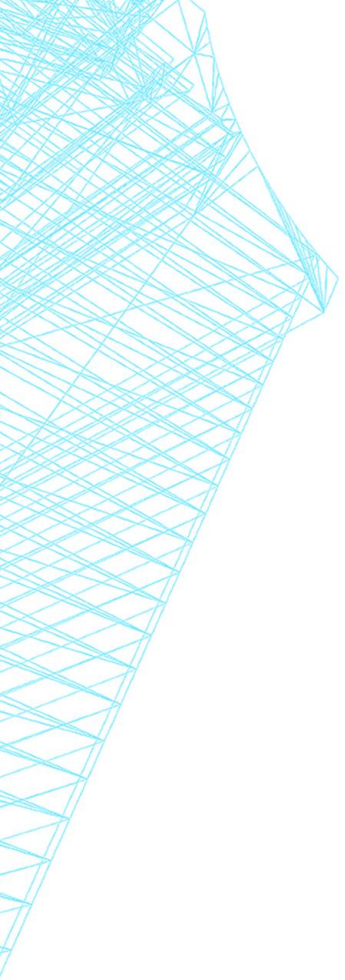
**Wesley Johnson, IT Support
Daviess County Public Library**





A FEW DEFINITIONS, VIA DICTIONARY.COM

- Malware - software that is specifically designed to disrupt, damage, or gain unauthorized access to a computer system.
- Spyware - software that enables a user to obtain covert information about another's computer activities by transmitting data covertly from their hard drive.
- Adware - software that automatically displays or downloads advertising material (often unwanted) when a user is online.
- Ransomware - a type of malicious software designed to block access to a computer system until a sum of money is paid.





IN THE SUMMER OF 2019...

- One of our Circ-It self-check stations white-screened, then they all did
- White screen = loss of communication with server
- A message like the one on the next slide appeared on all self-checks
- Infection spread to our entire staff network; Polaris server included
- Our most recent backups were unusable
- My boss was unable to watch the Game of Thrones finale at his house



Ooops, your files have been encrypted!

English

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?

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

CMT from Mondays to Fridays

Payment will be raised on

5/16/2017 00:47:55

Time Left

02:23:57:37

Your files will be lost on

5/20/2017 00:47:55

Time Left

06:23:57:37

[About bitcoin](#)

[How to buy bitcoins?](#)

[Contact Us](#)



Send \$300 worth of bitcoin to this address:

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Copy

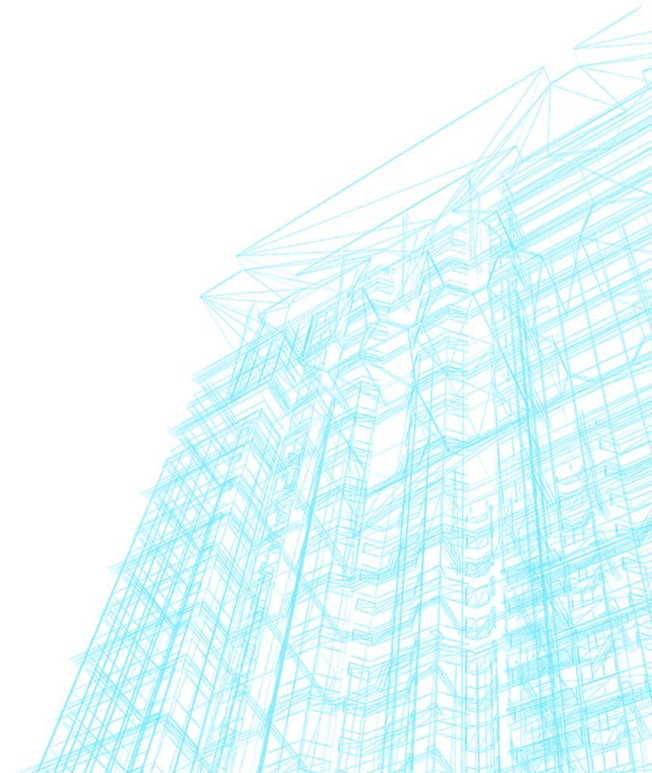
Check Payment

Decrypt

- We scanned, we talked to reporters, we re-imaged when needed, we talked to reporters, we deleted files, rebuilt our catalog from scratch, we talked to reporters, and we talked to reporters
- Once we went back online, we were hit again by the same infection
- Then we were hit with a different infection
- **We then decided to redo every computer in the building and re-scan every archived file**

FIRST STEPS

Stress Level = 100%





SHOUTOUTS

- **Henderson County**, our neighbors, loaned us staff to help re-catalog every item over the course of two days
- The fine folks at **Bibliocommons**, after I asked if it was possible, figured out a way to export MARCs from their last-known good version of our catalog to send to us. This saved a TON of work.



A DIFFERENT APPROACH

- The mass wiping of our PCs gave us a great opportunity to upgrade to Windows 10. Windows 7, which reached EOL the next year, was in use on many staff PCs.
- Replaced our Fortinet Firewall with a Sophos XG 230 security appliance – firewall, VPN, Endpoint Protection (replaced previous a/v)
- Adopted Ninja RMM service – remote support (great for COVID-era), update automation, & more
- Subscribed to KnowBe4 Security Training



DEEP FREEZE

- A “freeze” of the computer is taken after setup. Essentially a snapshot of settings, programs, etc.
- Each computer reverts to the “freeze” after it’s rebooted – anything, malicious or not, saved to the computer between reboots is wiped
- A “thawed space” can be set up on each hard drive if there are user files that need to remain on the drive. Perfect if DF is used on staff PCs
- “Thawed” periods can be scheduled for weekly updates
- Our network is in Public and Staff segments. DF is only on Public PCs. Our Publics have had ZERO outbreaks.



HAVE SOLID BACKUPS

- Backup often and to multiple sources – cloud and physical
- At least one off-site source, more if possible
- An off-site source detached from the network is protected from future infections
- Frequently check your backups to ensure they're healthy

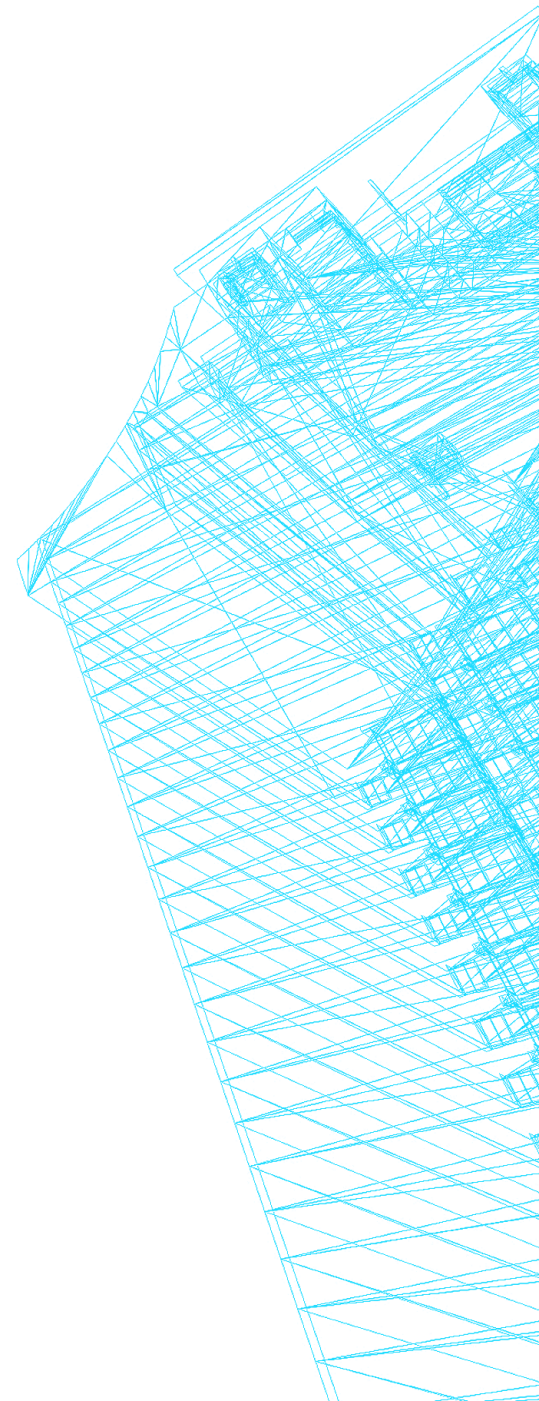


SECURE REMOTE DESKTOP, OR DON'T USE IT

- Remote Desktop is an incredibly easy way to compromise computers
- Make sure it's SECURED if it's enabled on your hardware firewall
- We suspect a flaw in RDP is what allowed our network to be compromised

AFTER THE WIN 10 UPGRADE...

we enabled Microsoft's beefier security tools in Windows
10



CONTROLLED FOLDER ACCESS + DATA RECOVERY

Ransomware protection

Protect your files against threats like ransomware, and see how to restore files in case of an attack.


Controlled folder access

Protect files, folders, and memory areas on your device from unauthorized changes by unfriendly applications.



Ransomware data recovery

You may be able to recover files in these accounts in case of a ransomware attack.

 Set up OneDrive for file recovery options in case of a ransomware attack.


Set up OneDrive

[Dismiss](#)

Microsoft OneDrive ×

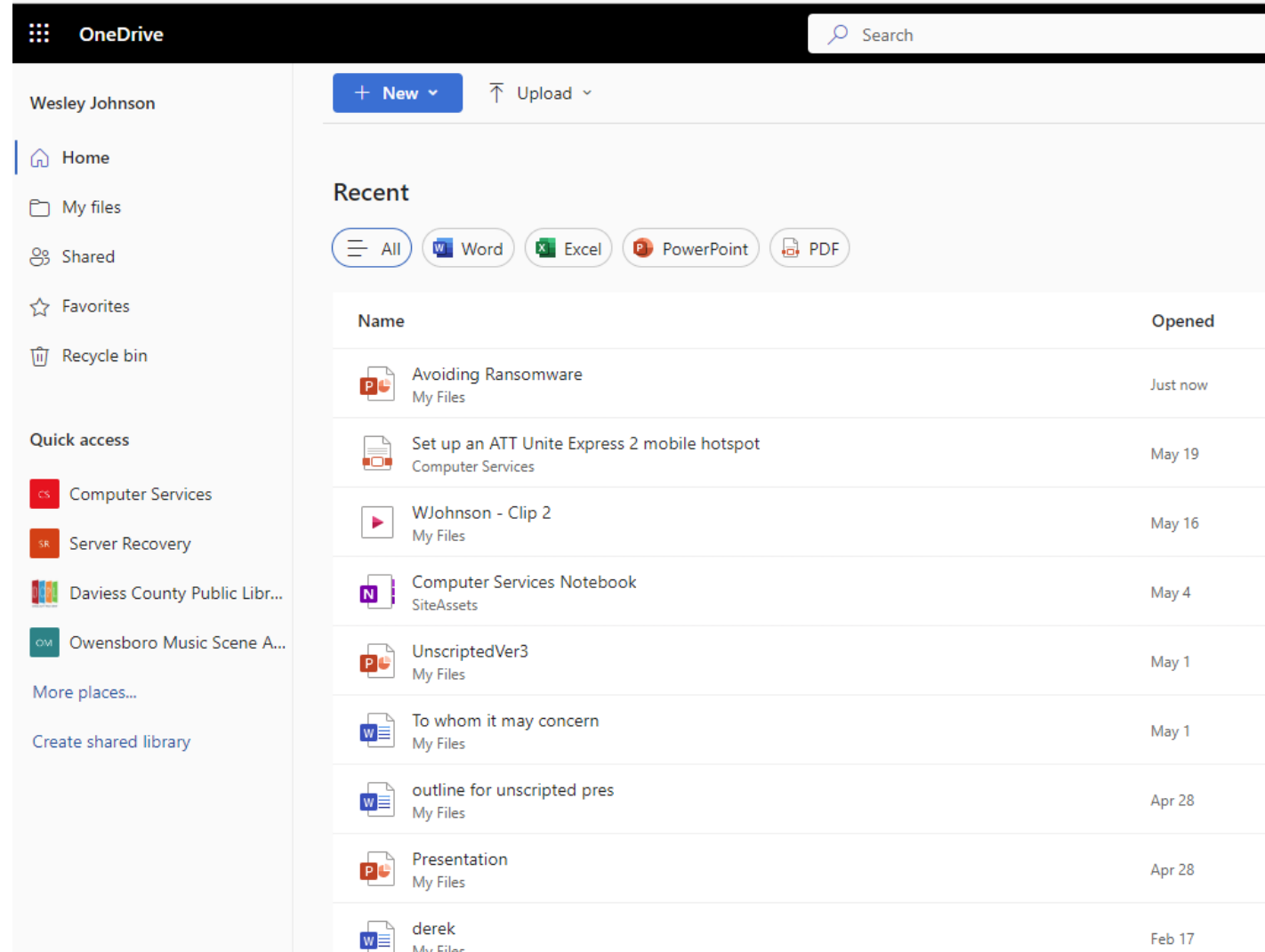
Set up OneDrive

Put your files in OneDrive to get them from any device.












Email address ⓘ

DATA RECOVERY VIA ONEDRIVE



The screenshot shows the OneDrive web interface for user Wesley Johnson. The left sidebar contains navigation options: Home, My files, Shared, Favorites, Recycle bin, Quick access (with links to Computer Services, Server Recovery, Daviess County Public Libr..., and Owensboro Music Scene A...), More places..., and Create shared library. The main area features a 'Recent' section with a filter menu (All, Word, Excel, PowerPoint, PDF) and a table of files.

Name	Opened
 Avoiding Ransomware My Files	Just now
 Set up an ATT Unite Express 2 mobile hotspot Computer Services	May 19
 WJohnson - Clip 2 My Files	May 16
 Computer Services Notebook SiteAssets	May 4
 UnscriptedVer3 My Files	May 1
 To whom it may concern My Files	May 1
 outline for unscripted pres My Files	Apr 28
 Presentation My Files	Apr 28
 derek My Files	Feb 17



MICROSOFT ANTI-VIRUS

- Impressive and robust, especially for a free tool
- Protects against viruses AND ransomware
- Updating and scanning is unintrusive
- We continued using Microsoft A/V until we acquired our Sophos firewall and Sophos Endpoint Protection
- It's great for smaller networks, but, if budget allows, going with something beefier is recommended

KNOWBE4 FREE TOOLS



PRODUCTS & SERVICES ▾ FREE TOOLS ▾ PRICING ▾ RESOURCES ▾ ABOUT US ▾ CONTACT US ▾

Our ransomware simulation tool will find out how vulnerable your network is to common ransomware and cryptomining attacks.

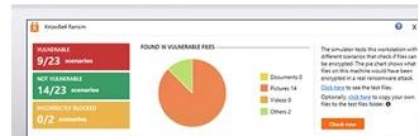
Is your network effective against ransomware infections when employees fall for social engineering attacks?

KnowBe4's Ransomware Simulator "RanSim" gives you a quick look at the effectiveness of your existing network protection.

RanSim will simulate **22 ransomware** infection scenarios and **1 cryptomining** infection scenario and show you if a workstation is vulnerable.

How the RanSim Simulator works:

- 100% harmless simulation of real ransomware and cryptomining infections
- Does not use any of your own files



I want my **RanSim** download

First Name*

Last Name*

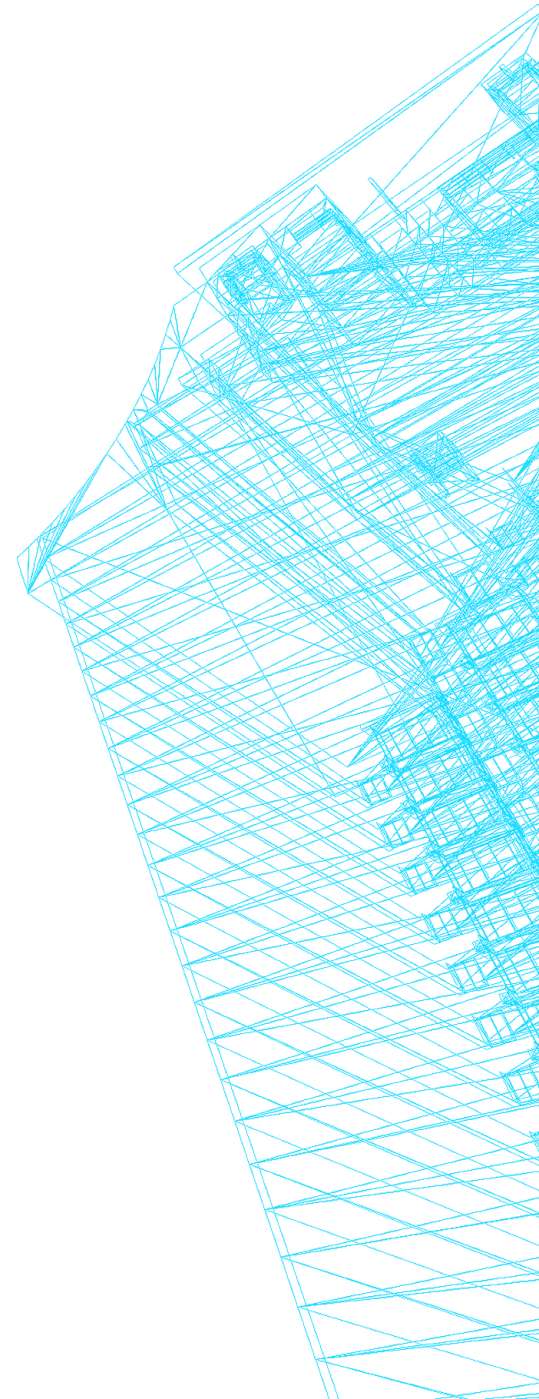
Business Email*

Company Name*

Phone*

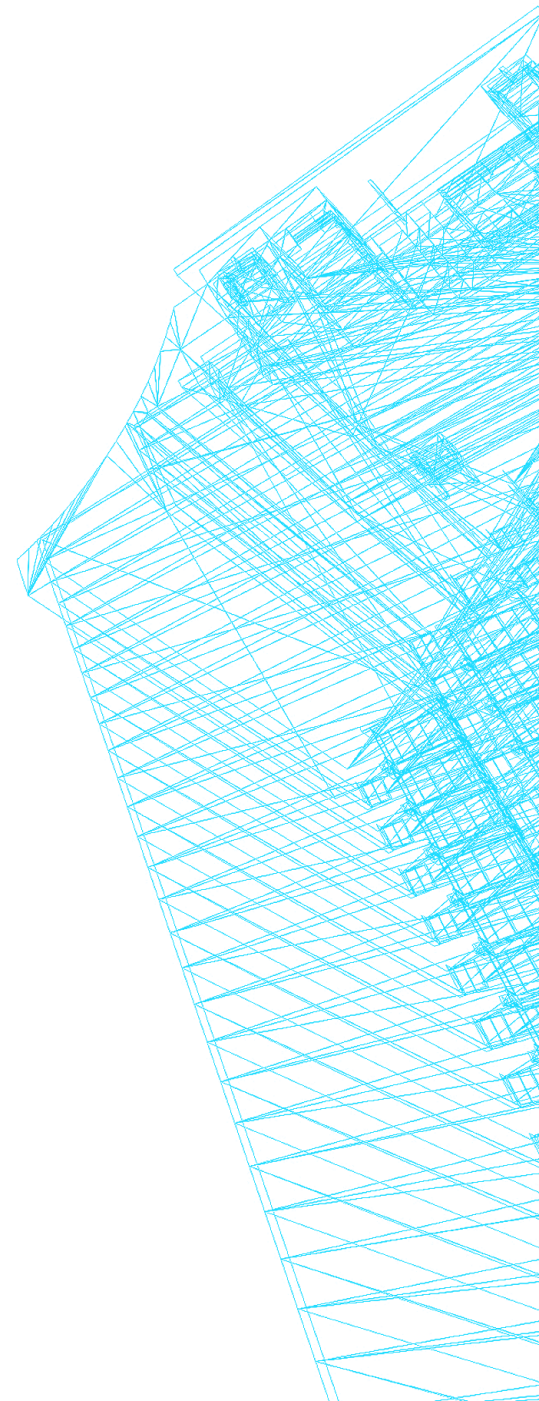
STAFF TRAINING

KnowBe4 Premium offers amazing, engaging content to help keep your staff sharp



HIGH-END GEAR

I'll now demonstrate some of the high-end things we eventually adopted to keep our network secure





FILE UNDER NOT FREE, BUT WORTH IT

- NINJA RMM – Robust remote management with lots of great options to help you prevent, troubleshoot, and fix tech issues. It also functions as an inventory – every item on your network will have a profile created for it – NinjaOne.com
- Sophos XG230 – Security appliance with a hardware firewall (AMAZING web filtering) and Sophos Endpoint Protection (A/V). Admins are alerted as soon as an infection is detected – Sophos.com
- KnowBe4 – Exercises, quizzes, fake phishing emails, videos (Inside Man is GREAT – staff was VERY engaged by this), and more. We have our leaderboard enabled so it’s gamified. - KnowBe4.com
- Deep Freeze – Keeps computer in a “frozen” state. After a reboot, it reverts to that state, getting rid of all personal files and infections – Faronics.com



THANKS!

I love talking about this stuff! Feel free to reach out if you think of any questions after the webinar has ended

Wesley Johnson
Daviness County Public Library, IT Support
wjohnson@dcplibrary.org