

2021 Steven W. Rhodes Consumer Bankruptcy Conference



Rich Collins
Manager of Information Services
Office of David Wm. Ruskin
Standing CH 13 Trustee, Detroit
rich@det13.com

IT NIGHTMARES: The Human Firewall

This document is intended to provide more detailed information and supplement the informal talk during the presentation. The SharePoint slide appears at the top of each section of detail.

Our offices are connected to each other via email and the documents we share. The weakest security in our community is our greatest point of vulnerability.

THAT is a nightmare!

Each employee in our bankruptcy community is a “Human Firewall” that helps protect the rest of us.

The following information is provided to help identify areas of concern and how to address them.

First, some
dreams!



I would be remiss to pass up this opportunity to talk about some of the tools available to the Chapter 13 community that help make life easier for everyone involved.



DET-BK Email list:

Enrollment form is at this link:

https://www.det13.com/tasks/sites/chap13/assets/file/FORM_DET13_LISTSERV_ENROLLMENT_401.0821.pdf

The DET-BK email list is more than just the Chapter 13 Trustees posting docket information. This list is open to discussion on ALL aspects of consumer bankruptcy in the Eastern District of Michigan, particularly the Southern Division. There are members on the list who practice in the Northern Division as well. Besides docket info, some topics that have been discussed include:

- Actual v Constructive Notice for omitted creditors
- Mortgage modification issues
- PPP Loan issues
- NextGen PACER issues
- Appraisal service recommendations
- The future of court hearings discussions
- Issues related to interacting with Federal Agencies
- Child Care Tax Credits
- Evaluation of bankruptcy software programs

These are issues that touch on all aspects of consumer bankruptcy and can help every office expand their toolkit of resources when a problem issue arises. If you aren't a member join now! If you are a member, thank you and keep posting!

Carl Bekofske's office also maintains an email list for matters in their area. Please email sskutt@flint13.com to get information about joining their list.

The Email Reader Replacement – 13Documents!



The Ch 13 Trustees of the Eastern District of Michigan have used the “Financials Email Reader” program to receive case documents that are not filed with the court. The base program behind the Email Reader has not kept up with modern standards and will not be upgraded or replaced by the company that makes it. We feel that it is time to move on.

13Documents is the document portal program we have started using.

13Documents is used by many Ch 13 Trustee offices around the country, including Michigan and Ohio.

The advantages of 13Documents:

- Encrypted transmission from your office to ours.
- Free for you to use.
- 25mb file size (up from 10mb with the email reader).
- Up to 10 files uploaded in a batch (up from 1 file per email).
- View a history of all files uploaded to 13Docs and the status of our download of those documents.
- More document types to choose from (up from 1 document type for all documents).

We hope to be able to terminate the old Financials Email Reader by the start of 2022.

National Data Center

The National Data Center (www.NDC.org) is an organization created by the National Associations of Chapter Thirteen Trustees to facilitate access to information for Creditors, Debtors and Debtor Attorneys. They have many tools that can help each of these parties to manage their Chapter 13 Cases.

- Payment vouchers at a click.
- Data from nearly every Ch 13 Trustee across the country via ONE login (the 13Network and other services require separate logins for each Trustee).
- Libraries of documents related to the case.
 - The annual Tax letters and Periodic Reports can be found online at any time. No more paper!
- Reports that can be run on demand or sent to you on a regular basis.



rich1@det13.com | [Sign Out](#) | [Overview](#) | [Get Help](#)

A screenshot of the National Data Center web application. The top navigation bar includes links for Overview, Portfolio, Vouchers, Trustee Data Status, Reporting (which is highlighted), and Settings. A search bar on the right contains the text 'Example: 1101234'. Below the navigation bar, there are tabs for My Reports, Dashboard Reports, Enterprise Reports (which is selected), and Subscriptions. The main content area is titled 'Enterprise Reports' and contains a list of report categories, each with a calendar icon and a brief description: 'Attorney Payee' (Itemizes any claims where the payee is the Debtor Attorney...), 'Attorney Portfolio Active Cases' (Portfolio cases that have an NDC_Case_Status of "Active-Open".), 'Attorney Portfolio Active Unconfirmed Cases' (Portfolio cases that have an NDC_Case_Status of "Active-Open", but no Confirmed_DT.), 'Attorney Trustee Payments' (Attorney payments recently made by Trustees.), 'Debtor Attorney Portfolio 362 Dockets' (Cases having a docket entry with "362" in it.), 'Debtor Attorney Portfolio Confirmed Cases with Mortgage Arrears' (Confirmed cases having a secured claim for arrears.), and 'Debtor Payment' (Displays case data for last payment date, and calculates the days from the last payment until today). At the bottom of the list is a section for 'Custom Reports'. A button labeled 'GIVE FEEDBACK ON REPORTING' is located in the top right corner of the report list area.

These reports can help debtor attorneys keep track of how much they are owed on cases, cases that are becoming delinquent and more.

Contact me if you wish to become enrolled with the NDC! Get your clients to enroll with the NDC when you prepare them for the 341! Have them visit www.ndc.org to register.

Welcome To My Nightmare



Unlike Alice Cooper's nightmare, I don't think you'll like it in my nightmare – but hopefully this presentation will generate some ideas to help your office and, as a result, help our entire community to be more secure.

Email is the most common way for attackers to gain access to your computers. Attachments and links in emails are the way they trick you into installing malware yourself. Our community shares many emails and documents with each other. We have seen instances over the years where an office appears to have sent out a document share that was really sent by someone else. The following information is provided to help everyone create best practices that will help protect us all.

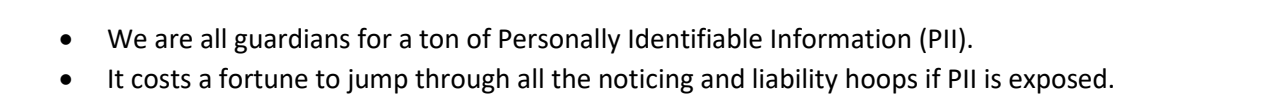
Working from Home



Even before the pandemic many offices had started to allow employees to work from home at least part of the week. The pandemic itself forced us all to evaluate how to handle permanent work from home scenarios. Here are some things to think about when allowing staff to work from home:

- Do you have a policy or agreement for employees that work from home?
 - <https://blog.vantagecircle.com/work-from-home/>
- Do you have a system in place to manage software updates and provide remote support?
 - <https://www.manageengine.com/products/desktop-central/>
 - <https://docs.microsoft.com/en-us/windows-server/administration/windows-server-update-services/get-started/windows-server-update-services-wsus>
 - <https://support.microsoft.com/en-us/windows/solve-pc-problems-over-a-remote-connection-b077e31a-16f4-2529-1a47-21f6a9040bf3>
- Are your employees working in a private area?
- Are your employees banned from printing?
- Are your employees using a secure method to connect to your office?
 - See section below on VPN.
- Are your employees maintaining safe practices on the computer?
- Have you encrypted the hard drives of any devices leaving the office?
 - <https://docs.microsoft.com/en-us/windows/security/information-protection/bitlocker/bitlocker-overview>
- Do your remote workers have a TPM module on their out of office devices?
 - <https://whatis.techtarget.com/definition/trusted-platform-module-TPM>
 - These are questions everyone should be asking about remote workers.

- Some Work From Home Best Practices:
 - Organize your workspace. When your workspace is organized, you're less likely to misplace important documents and will have a place to put these documents when you aren't using them.
 - Follow your organization's policy for taking screenshots or pictures of sensitive information. Blur out any personally identifiable information (PII) or other sensitive information.
 - Note that just using a photo program to "blur" a document does not mean you have redacted the PII!
 - Be careful when posting company information on social media platforms such as LinkedIn. Even if the information seems harmless, it's better to review your organization's policy before posting.
- Protect your devices with strong passwords.
 - Set up passwords or passcodes to protect your devices. If you don't use passwords, cybercriminals can easily gain access to your devices should you lose them.
 - Use passphrases instead of a password.
 - "RhodesSemin@r2021!" is a better password than "Qrz1!5Rd3" because it has the same complexity but is easier to remember and is longer.
 - Don't use identical or similar passwords for multiple accounts. If you have trouble remembering your passwords, use a password manager to create and manage the passwords for your accounts.
 - Change the password for your Wi-Fi router. Most routers come with default passwords that can be easily guessed.
- Use appropriate equipment.
 - Follow organization policy when using work equipment at home. It's important that you use equipment provided by your organization as it may include important security measures to prevent cyberattacks.
 - If you're allowed to use personal devices for work, create a separate user profile for work. It's best to separate your personal and work profiles.
 - Don't download unnecessary applications or software onto your organization's devices. If you have questions about approved applications or software, review your organization's policy or ask your IT department.



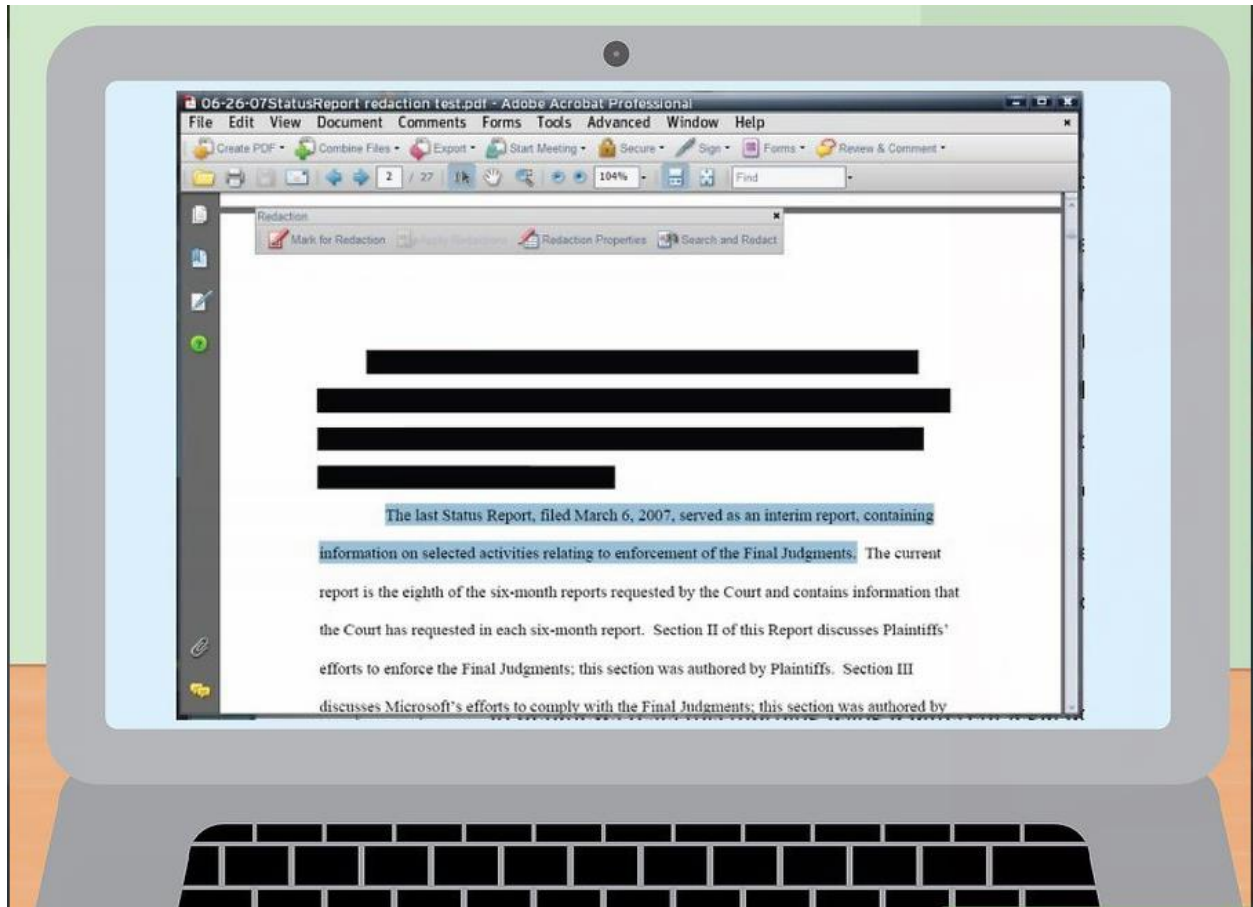
<https://www.dhs.gov/easy-request-legal-status/> that personally identifiable information

Scouring Bill in a Work-From-Home World

<https://www.vernypossible.com/insights/playbook-for-secure-remote-work-during-covid-19-and-beyond>

Data breach notification laws

Redacting PII



Many of us were taught to use a PDF mark up tool to cover up PII and then use a “flatten” option to cover up the PII. It turns out that this doesn’t work!

In 2020 there was a discussion on the DET-BK list on this subject and we worked through different scenarios.

- Adobe now charges extra for a “Redaction” tool for Acrobat Standard.
 - If you use a markup tool to cover PII it can still be viewed with a number of different tools built in to Acrobat Standard.
- Using the “Print to Adobe Acrobat” option DOES NOT protect the PII covered by a markup tool.
- Using “Print to Microsoft PDF” DOES seem to work, but not every computer will have this option.
- Other PDF programs have built in redaction tools and do not charge extra for them.

Phishing



- Phishing is when the bad guys contact people with via email to lure them into clicking on a link or opening a file.
 - Your information is available on the internet. Your office structure, your email addresses, your job titles – all of this is available to the most casual of hackers. This makes it easy of the bad guys to impersonate you or anyone in your office or people you commonly deal with.
- Make your emails distinct so that people have a better idea that it is truly from you:
 - Include the name of the recipient as a “salutation”.
 - Use complete sentences and make specific references to any attachments.
 - Do not send, “Here is the document we’ve discussed.”
 - Do send, “Here is the stip on the Smith case, 55-10000, that we have been discussing.”
 - Always include a case number in the subject line.
- Train your staff on how to recognize phishing attempts and improve overall computer security.
 - [Know Be 4](#) and [Breach Secure Now](#) are two similar resources that provide a wealth of training materials for your staff. Your anti-virus or firewall vendor may have something as well, like Trend Micros’ Phish Insight program.
 - The material is presented in an “Infotainment” manner to make the material more impactful.
 - Services like these also provide analytical review of your staff to determine areas of training individuals may require.
 - The emphasis is on the “human firewall” – each of us are the last barrier between the bad guys and our computer systems.
- There are variants called “Vishing”, which uses phone calls to lure people into executing malicious software, and “SMishing” – using text messages to compromise a user’s phone.

- Sample Phishing email:
- https://office-watch.com/2021/inside-a-real-microsoft-365-phishing-attack/?utm_medium=Email&utm_source=ow Sample Phishing Vendor Training programs:

855-KnowBe4
Blog
Support
Partners
Request A Demo
Account Login

KnowBe4
Human error. Conquered.

PRODUCTS & SERVICES
FREE TOOLS
PRICING
RESOURCES
ABOUT US
CONTACT US

FORRESTER RESEARCH
THE FORRESTER WAVE™
Security Awareness And Training Solutions
Q1 2020

Challengers: Stronger content offering, Weaker content offering, Weaker strategy, Market presence

Contenders: Evolve security, Protonmail, Microsoft, Malware, KnowBe4, PhishLabs, Medallia, Cofense

Strong Performers: KnowBe4, Protonmail, Microsoft, Malware, KnowBe4, PhishLabs, Medallia, Cofense

Leaders: KnowBe4, Protonmail, Microsoft, Malware, KnowBe4, PhishLabs, Medallia, Cofense

KnowBe4 Named a **Leader** in The Forrester Wave™: Security Awareness and Training Solutions, Q1 2020

» Download Your Complimentary Copy of the Report

Here, have a cookie! See our [Privacy Policy](#) to learn more.

If you'd rather, your information won't be tracked when you visit this website. A single cookie will be used in your browser to remember your preferences not to be tracked.



The Inside Man: Season 1 Episodes 1-12

Video Module



PII and You

Training Module



Social Media: Staying Secure in a Connected World

Training Module



2020 Common Threats

Training Module

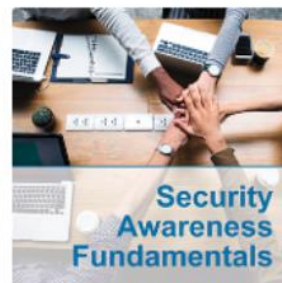
Foundational



Security Awareness Proficiency Assessment



Gatekeepers: Protecting Private Information and Access




Security Awareness Fundamentals


Training Module



2019 Kevin Mitnick Security Awareness Training - 15 min



[Home](#)
[Blog](#)
[Products](#)
[Partner With Us](#)
[About Us](#)
[Contact Us](#)



THE BEST MSP-FOCUSED END-USER EDUCATION PLATFORM

Manage the Weak Link in Security: *Humans*

Unparalleled insight with our Employee Vulnerability Assessment

Start Free Trial →

[Phishinginsight.trendmicro.com](https://phishinginsight.trendmicro.com)



Services ▾


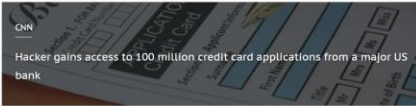
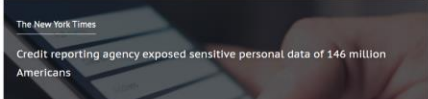



Empower your employees to detect threats and protect your organization

Phish Insight enhances information security awareness for your organization by empowering people to recognize and protect themselves against the latest threats.

Try for Free Now →

What do these news stories have in common?

 <p>The Verge Tech giant targeted in \$50 million ransomware attack</p>	 <p>CNN Hacker gains access to 100 million credit card applications from a major US bank</p>
 <p>The New York Times Credit reporting agency exposed sensitive personal data of 146 million Americans</p>	 <p>Business Insider Phone numbers and personal data of 533 million social media users leaked online</p>

→ Human Error

Security Webinars:

<https://www.knowbe4.com/webinar-library>

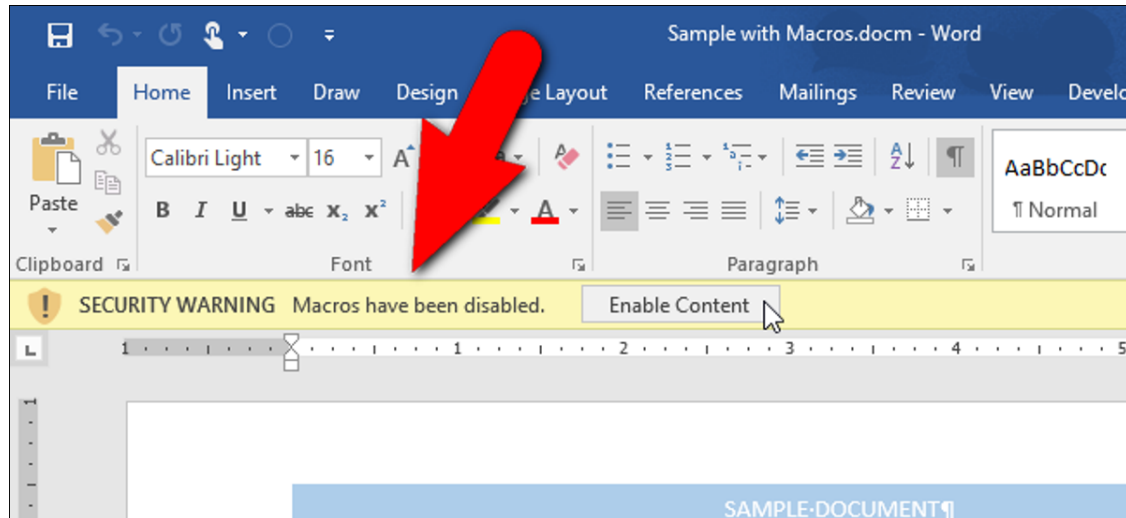
There are free training videos at this site, along with their current lineup of free security webinars.

Email security

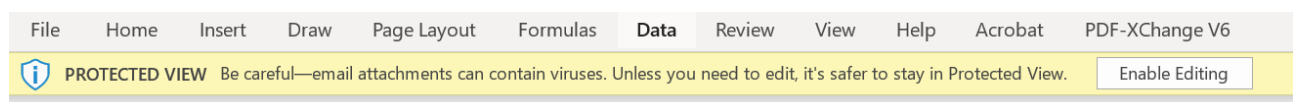


- Free is not necessarily better when it comes to email. Many of the free email vendors are routinely hacked.
 - Recognizing a hacked Yahoo account:
<https://ph.help.yahoo.com/kb/answers/recognize-hacked-yahoo-mail-account-sln2090.html>
 - One billion Yahoo accounts hacked:
<https://www.industryweek.com/technology-and-iiot/article/22006110/latest-yahoo-hack-is-the-largest-data-breach-to-date>
 - Outlook.com hack worse than reported:
<https://www.itpro.com/security/33454/outlookcom-hack-much-worse-than-initially-thought>
 - Account info for millions of Gmail accounts stolen:
<https://www.express.co.uk/life-style/science-technology/1448712/Millions-of-Gmail-Facebook-Amazon-logins-STOLEN-find-out-if-you-are-affected>
- Look into using an email platform that allows Multi Factor Authentication (see below). MFA is a step towards making sure that you (or your staff) are truly the only ones using that email account!
 - If you are using Microsoft's Exchange Online then they have an easy to use system for implementing MFA for all your users.
 - If you aren't using Exchange Online and Office/Microsoft 365 then you should seriously look into it. There are a number of tools you get with these services for free that would be otherwise unavailable or cost extra.
- Free anti-virus is not good anti-virus for the working world!
 - I recommend the site www.av-comparatives.org for an analysis of how well various products work in real world testing.

Document Security



In Microsoft Office products, Macros are little scripts that automatically execute functions. This could be as simple as automatically reformatting a pleading to pulling in data from another source. Because this function can execute commands it should be **TURNED OFF** until needed. Train your staff to NEVER “Enable Content” for a document that arrived from outside your office. If you do get a document that has this warning contact the originating office to make sure that they are aware that they sent a document with macros in it. They should be stripping the macros out before sharing it with others.

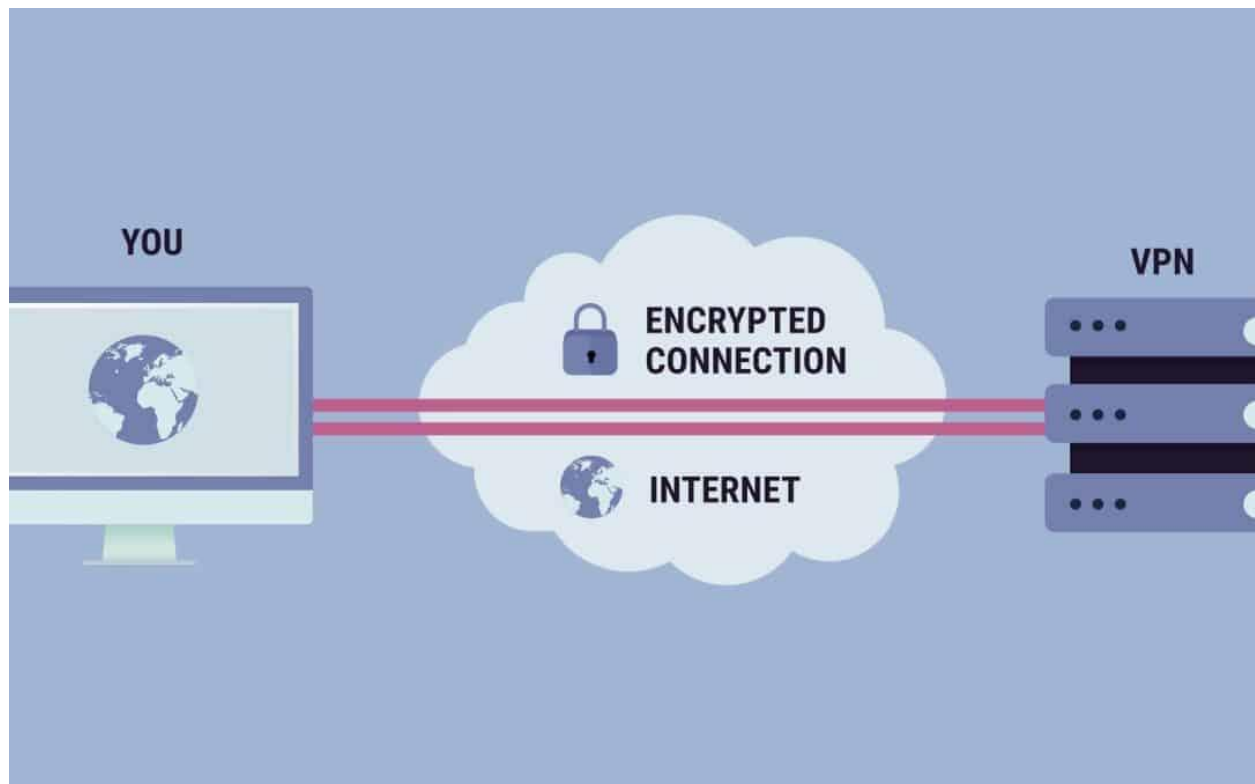


“Protected View” is different from macros. This warning in Office products is to alert you that the file came from an internet source. Many features of the Office products will be disabled while this banner is on display. This is to protect you until you can confirm that the document is authentic.

More information about Macros:

https://office-watch.com/2021/the-danger-still-lurking-in-excel-and-how-to-stop-it/?utm_medium=Email&utm_source=ow

VPN



- VPN stands for Virtual Private Network. It encrypts your data across the internet, making it secure from all but the most determined of hackers.
- If your office is working from home, working from court, or from anywhere outside of the office walls then they should be connecting using a VPN.
 - Free is not better in this instance. Many of the free VPNs have been found to not provide any actual security.
 - If you have computers connected to the internet in your office then you should have a firewall appliance. Your firewall should have a VPN client that works with it.
- If your staff are connecting to your office resources with a VPN then you are as secure as you can reasonably be for users outside of your office.
 - You can also use the VPN and your firewall as a web filter to make sure that your staff are not visiting risky sites while connected to your office.

Free VPN's lack security:

<https://securitytoday.com/articles/2018/09/26/free-vpns-are-a-privacy-nightmare-heres-why.aspx>

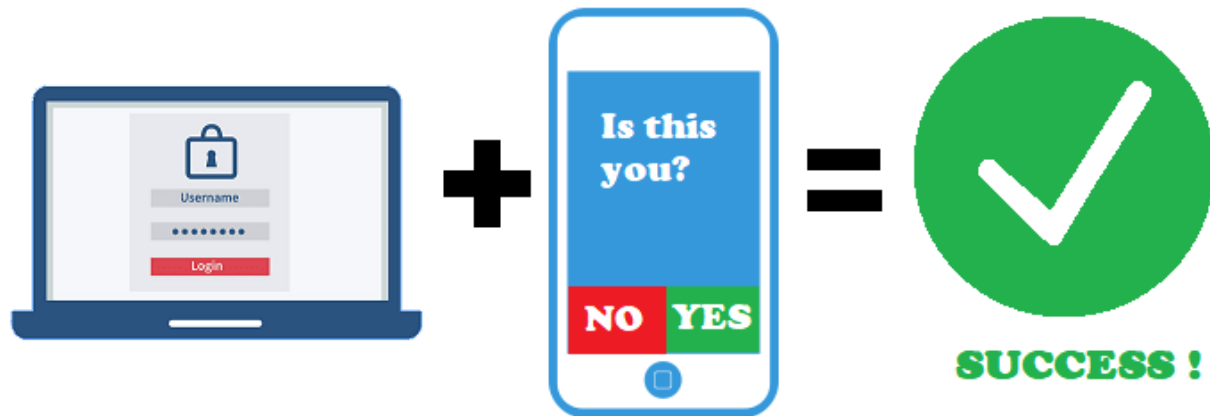
VPN services found recording user activity:

<https://securitytoday.com/articles/2018/09/26/free-vpns-are-a-privacy-nightmare-heres-why.aspx>

VPN servers found to lack encryption:

<https://arstechnica.com/gadgets/2021/07/vpn-servers-seized-by-ukrainian-authorities-werent-encrypted/>

Multi Factor Authentication



- Multi Factor Authentication (MFA, formerly 2FA)
 - Most of us are familiar with MFA when logging on to banks and other services. You enter your password and then use a separate code to prove that you're really you.
 - MFA is a means of making sure that the person connecting to your network is really that person. Because "brute force" password attacks against a network are so easy, a reasonably inspired hacker can crack any password on your network in less than an hour, often in just minutes.
 - An MFA system prompts the user to use a keyfob or app on their phone to input a code that only the holder of that device will have. A remote hacker using a brute force attack against your system won't have that code. Even if they get the password, they still can't get in.
 - You should NOT use an MFA system that sends a code via text message or an email. Both systems are easy to hack and thus are not really MFA. Tell that to your bank!
 - Google and Microsoft both offer free "authenticator" apps. Duo Security, which started in Ann Arbor and is now owned by Cisco, is free for fewer than 10 users.
 - MFA should be used for all employees to access company resources from outside the office. This should apply to logging in to a server over the VPN, utilizing Remote Desktop, accessing email and any cloud based resources the office uses (ie: SharePoint Online, Teams, Outlook, etc).
 - Note that cyber insurance carriers are now insisting that you utilize MFA to log on to ANY resource on your network – even from inside your office! This means each computer in your office, your servers, your switches... everything! If you have coverage you may want to check with your agent now to find out how to comply so that you can start budgeting.



1

The IT Nightmare



Our offices are all connected to each other via email and the documents we share with each other.

These are the two most common vectors that attackers exploit.

Each employee in our offices is a "Human Firewall" – the last and best defense against attacks on our systems.


2



3



4



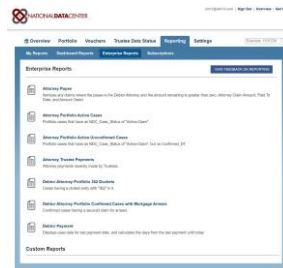
13 DOCUMENTS

Getting Started

The replacement for the Financials Email Reader

- We have begun moving users to 13Documents.com for required non-court filed documents.
- We hope to shut down the old email reader by the start of 2022.
- Other offices throughout the region already use it – check with your Trustee!

5



6

National Data Center

- Payment vouchers at a click!
- Access ALL the Ch 13 Trustees from ONE login!
- Reports and letters archived online instead of paper!
- Self run reports that can help you track YOUR financials
- Reports to keep track of delinquent cases

IT NIGHTMARES!



7




8

9

Redacting PII

10



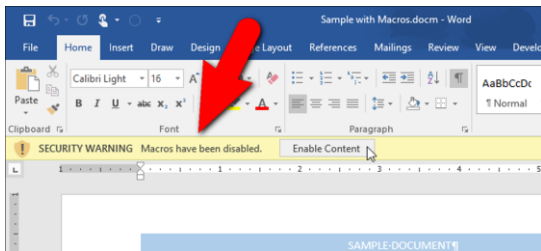
PHISHING

- To make your emails stand out from Phishing attacks:
 - Make your emails distinct and include the recipient's name.
 - Use complete sentences and make a specific reference to attachments.
 - Include a case number!

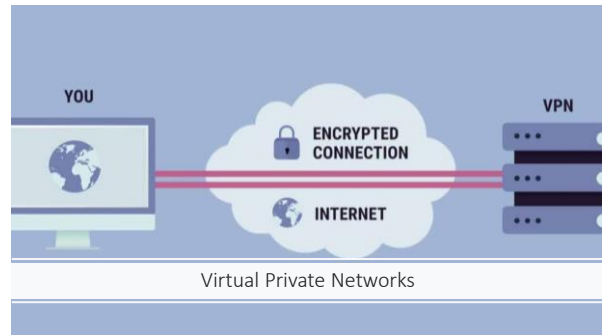
11

12

Document Security

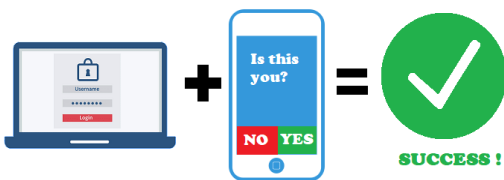


13



14

Multi Factor Authentication



15



16