

What do you need to know to better secure your business?

Isabelle Molamphy

M.S, CISSP, CISM

The background of the slide features several sets of thin, curved lines in light gray and blue, creating a sense of motion or a stylized globe. On the left side, there is a large blue speech bubble with a white outline, containing the word 'Agenda' in white text. The speech bubble has a small tail pointing towards the bottom left.

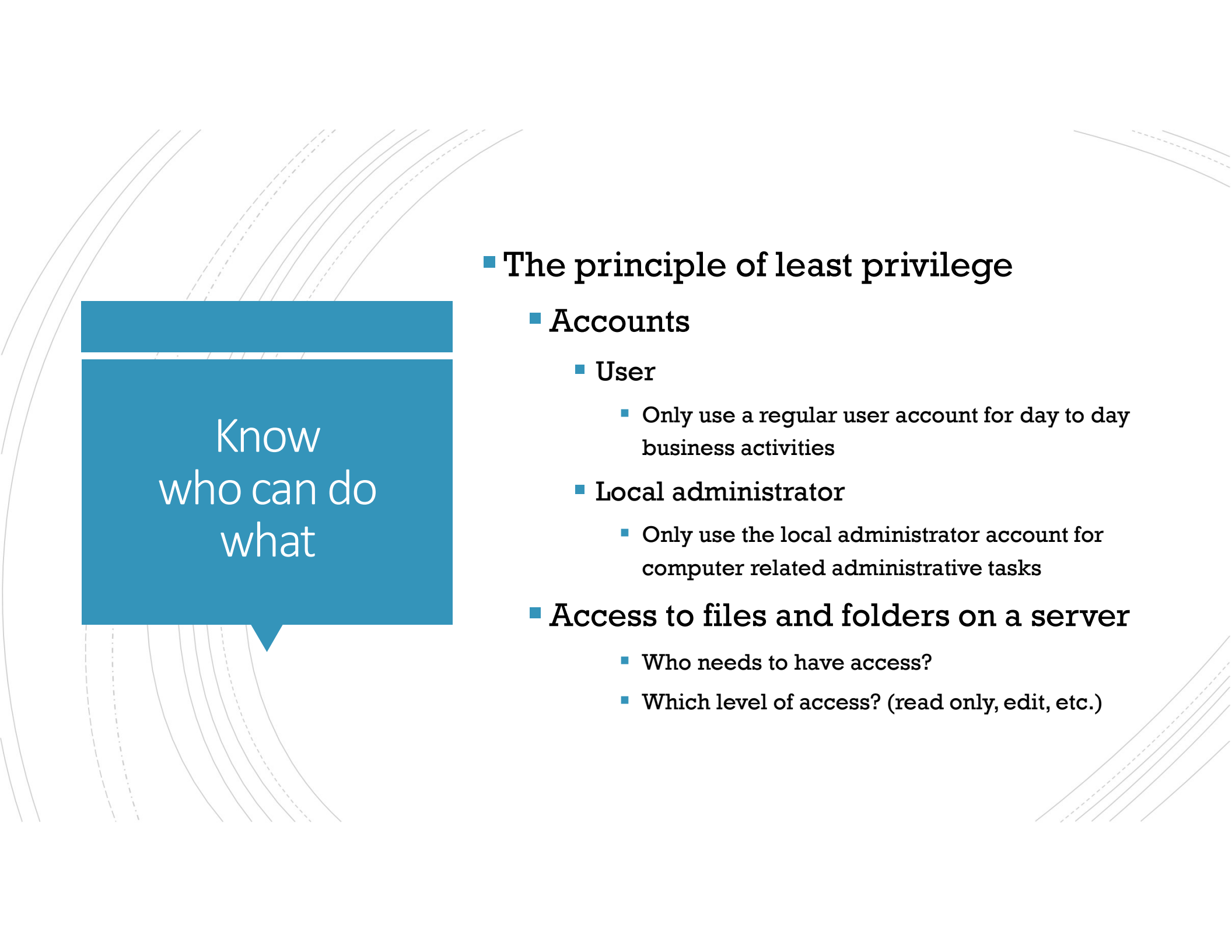
Agenda

- Know what you have.
- Know who can do what.
- Know how users authenticate.
- Know how vulnerable your assets are.
 - MBSA
- Know how far in time you will need your data.
- Know how to recognize a social engineering attack.

A decorative background featuring several thin, curved lines in shades of gray, some solid and some dashed, sweeping across the slide.

Know what you have

- **Identify critical information assets and where is the information stored**
 - On-premises
 - Is the data encrypted?
 - In the cloud (Box, OneDrive, etc.)
- **Inventory all hardware and software**
 - What devices are authorized to connect to the business network?
 - BYOD?
 - What types of connections does my business have?
 - Wired, wireless, VPN



Know
who can do
what

- **The principle of least privilege**
 - **Accounts**
 - **User**
 - Only use a regular user account for day to day business activities
 - **Local administrator**
 - Only use the local administrator account for computer related administrative tasks
 - **Access to files and folders on a server**
 - Who needs to have access?
 - Which level of access? (read only, edit, etc.)

Know
how users
authenticate

- Use unique complex passwords for each account
 - Password managers
 - (LastPass, LogMeOnce, etc.)
- When available, use Two-Factor Authentication (2FA):
 - Software based
 - Microsoft, Google, etc.
 - Hardware based
 - RSA, Yubikey, DUO, etc.



The background of the slide features several thin, curved lines in a light gray color, some solid and some dashed, creating a sense of motion or a globe-like pattern. On the left side, there is a blue rectangular box with a white text bubble shape at its bottom center.

Know
how vulnerable
your assets are

- **Set up Automatic Updates for:**
 - **Operating systems and Software**
 - **Install when prompted**
- **Scan for missing patches**
 - **Microsoft Baseline Security Analyzer (MBSA)(MS only)**
 - **Nessus**
- **Keep up to date on Anti-virus / malware**
- **Turn on the firewall on each of your systems**


Microsoft Baseline Security Analyzer

Microsoft Baseline Security Analyzer 2.3

Microsoft
Baseline Security Analyzer











Sort Order:





Security Update Scan Results

Score	Issue	Result
	SQL Server Security Updates	No security updates are missing. What was scanned Result details

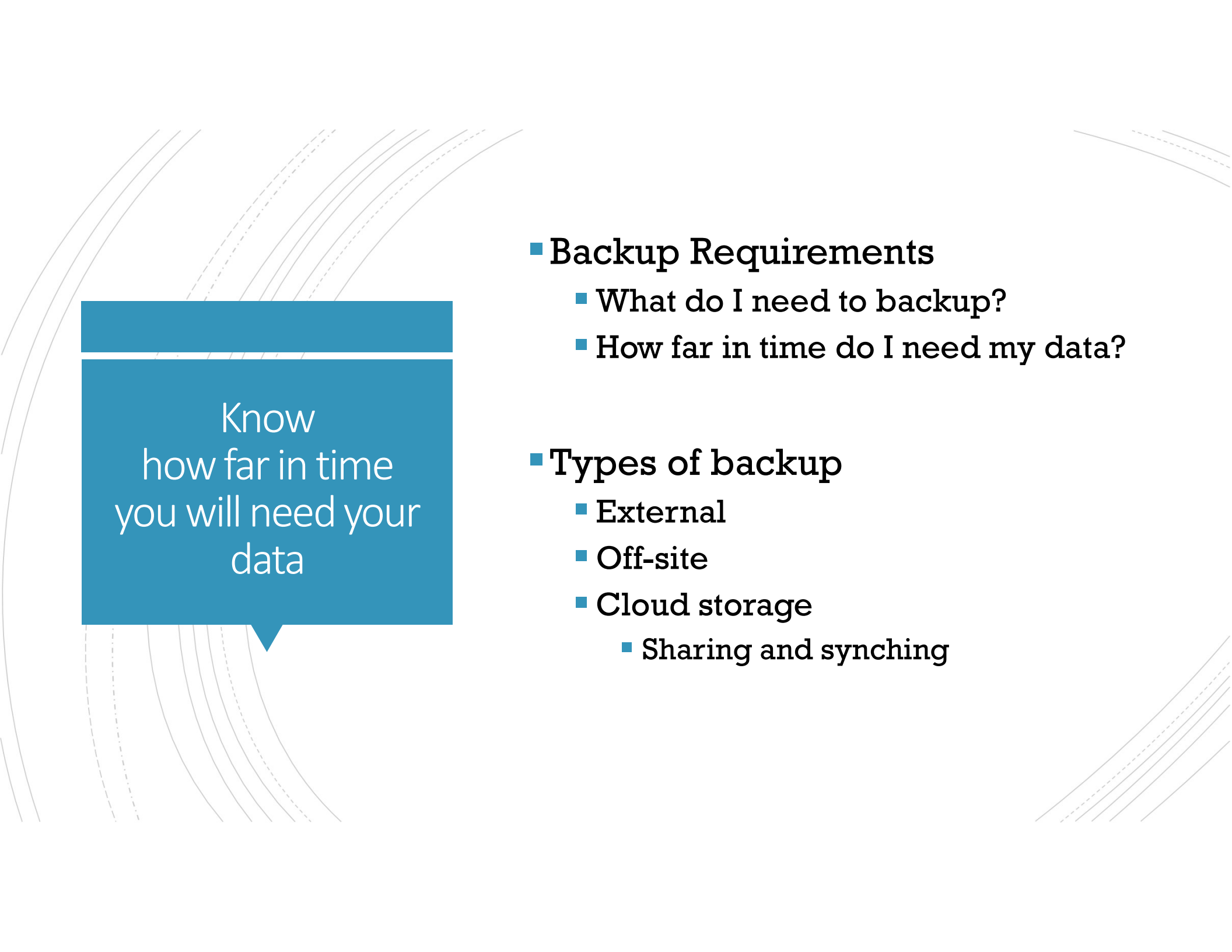
Windows Scan Results

Administrative Vulnerabilities

Score	Issue	Result
	Automatic Updates	The Automatic Updates feature has not been configured on this computer. Please upgrade to the latest Service Pack to obtain the latest version of this feature and then use the Control Panel to configure Automatic Updates. What was scanned How to correct this
	Password Expiration	Some user accounts (4 of 5) have non-expiring passwords. What was scanned Result details How to correct this
	Incomplete Updates	No incomplete software update installations were found. What was scanned
	Windows Firewall	Windows Firewall is enabled and has exceptions configured. Windows Firewall is enabled on all network connections. What was scanned Result details How to correct this
	Local Account Password Test	Some user accounts (4 of 5) have blank or simple passwords, or could not be analyzed. What was scanned Result details
	File System	All hard drives (2) are using the NTFS file system. What was scanned Result details
	Autologon	Autologon is not configured on this computer. What was scanned
	Guest Account	The Guest account is disabled on this computer. What was scanned
	Restrict Anonymous	Computer is properly restricting anonymous access. What was scanned
	Administrators	No more than 2 Administrators were found on this computer. What was scanned Result details

 [Print this report](#)  [Copy to clipboard](#)  [Previous security report](#) [Next security report](#) 

OK

The background of the slide features several thin, curved lines in a light gray color, some solid and some dashed, creating a sense of motion or data flow. On the left side, there is a blue rectangular box with a white border and a small triangular pointer at the bottom, containing the text 'Know how far in time you will need your data'.

Know
how far in time
you will need your
data

- **Backup Requirements**

- What do I need to backup?
- How far in time do I need my data?

- **Types of backup**

- External
- Off-site
- Cloud storage
 - Sharing and synching

Know how to
recognize a social
engineering
attack

- **Education**

- **Phishing, etc.**

- **Credential harvesting**

- **Ransomware**

- **Don't click on email links**
 - **Do not open attachments from unsolicited emails**
 - **Secure exchange of documents via Dropbox, Box...**

<https://www.consumer.ftc.gov/articles/0003-phishing>

<https://www.us-cert.gov/ncas/tips/ST04-014>

https://www.visasecuritysense.com/en_US/images/Visa_Phishing_02-23.pdf

<http://www.phishing.org/phishing-examples>

Phishing Statistics

- Phishing attempts have grown **65%** in the last year.
- **76%** of businesses reported being a victim of a phishing attack in the last year.
- **30%** of phishing messages get opened by targeted users and 12% of those users click on the malicious attachment or link.
- **95%** of all attacks on enterprise networks are the result of successful spear phishing.
- Phishing rates have increased across most industries and organization sizes — no company or vertical is immune.
- Nearly **1.5** million new phishing sites are created each month.

<https://blog.dashlane.com/phishing-statistics/>

Spear phishing process

```
graph TD; A[Research using public information] --> B[Email is sent]; B --> C[Email is opened because user 'knows' the user or originating company / agency]; C --> D[Link is clicked or attachment opened]; D --> E[Information is stolen or malware downloaded]; E --> A;
```

Research using
public information

Email is sent

Email is opened
because user
“knows” the user or
originating
company / agency

Link is clicked or
attachment opened

Information is
stolen or malware
downloaded

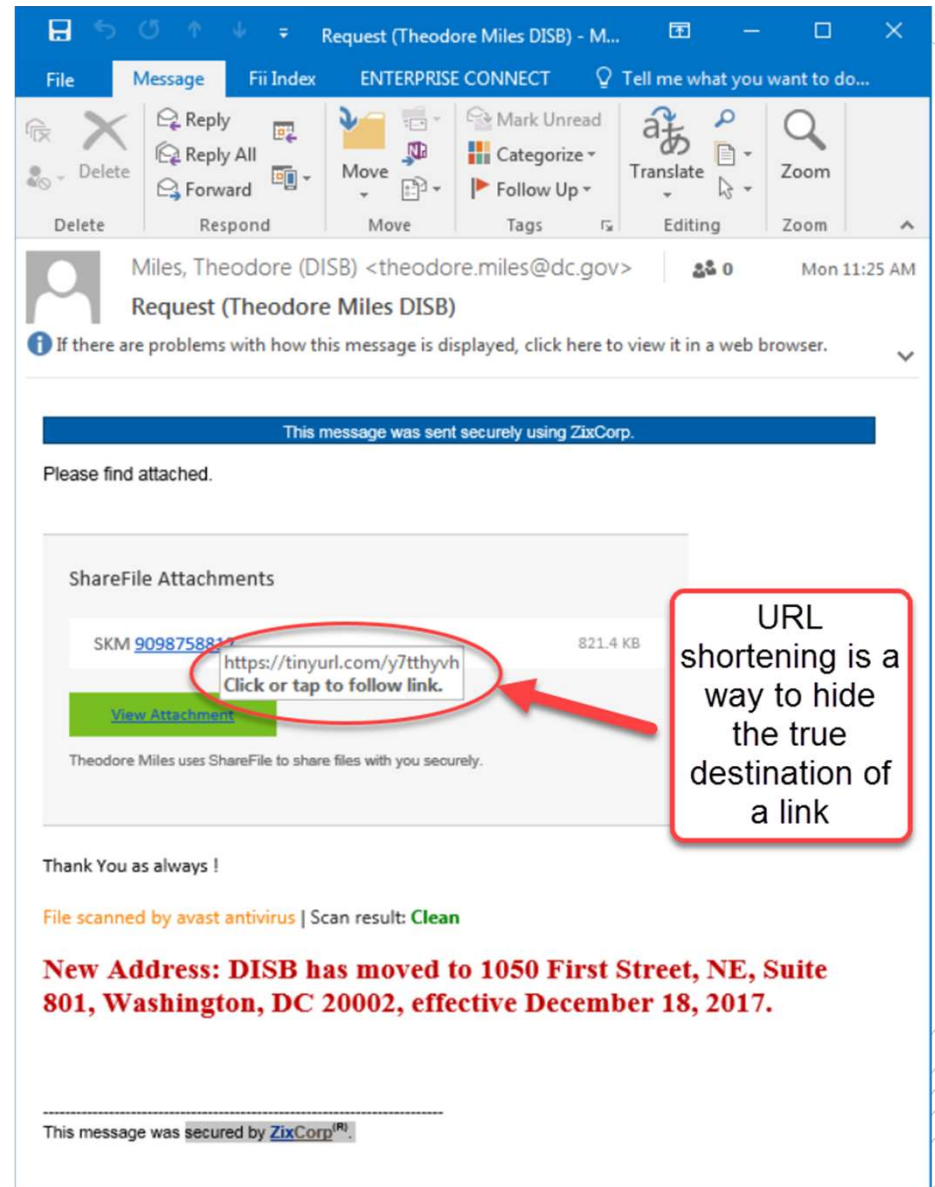


Phishing telltale sign

- Check for spelling/ grammar mistakes
- Analyze the salutation
 - Is the salutation “vague”? (valued customer, Dear User, etc.)
- Don't give up personal information
 - Think twice before typing your username and password
- Beware of urgent or threatening language in the subject line
- Review the signature
- Proceed with caution when email has attachments
- Don't trust the header from email address
- Don't believe everything you see

Unsolicited email

- DISB
- Compromised email
- No salutation
- Poor Presentation
- URL shortening - tinyurl.com
- No Signature block
- Encrypted email and virus free





What if you
clicked on the
link?

1. Disconnect from the network immediately.
 - Was it credential harvesting? Or malware?
2. Change your password immediately while logged on to a different computer.
3. Notify your IT support
4. Use system Restore if available
5. Depending on the situation, you may have to:
 - Notify your customers
 - Notify Law Enforcement
 - Notify cyber insurance
 - Notify the Attorney General

<http://www.atg.wa.gov/data-breach-notifications>

The background of the slide features several thin, curved lines in a light gray color, some solid and some dashed, creating a sense of motion or a stylized globe. On the left side, there is a large blue speech bubble with a white border. Inside the bubble, the text "In conclusion" is written in a white, sans-serif font. To the right of the bubble, there is a list of three bullet points, each preceded by a small blue square.

In conclusion

- Practice good cyber hygiene
- Implement principle of least privilege
- Think twice before clicking on a link or opening an attachment.

The background features a series of concentric circles in a light gray color, some of which are dashed. A solid blue speech bubble is centered on the page, pointing downwards. The text "Questions ?" is written in white inside the bubble.

Questions ?