

A PRACTICAL GUIDE FOR BUSINESS OWNERS AND THEIR TEAMS

CYBERSECURITY 101

A Jedi Field Guide for Your Business

Spot the trap. Protect the crew.
Keep the mission moving.

The full Connexiom Cybersecurity 101 training content, with Jedi Notes woven throughout. All 15 chapters, the detailed examples and checklists, glossary, and resources.

The Power to Connect and Control

October 2026 | Full-content Jedi edition

THE JEDI ARCHIVES

Table of Contents

About Connexiom	3
Are You Prepared for a Cyber Attack?	3
Introduction: The Need to Educate Employees on Cybersecurity	5
Chapter 1: Physical Security Precautions	7
Chapter 2: Email Threats	9
Chapter 3: Username and Password Management	11
Chapter 4: Mobile Security	14
Chapter 5: Secure Website Browsing	16
Chapter 6: How to avoid Viruses, Trojans, Worms and Spyware	18
Chapter 7: How to secure your data	20
Chapter 8: How to avoid SPAM	22
Chapter 9: How to avoid being Phished	24
Chapter 10: How to choose secure passwords	26
Chapter 11: How to be safe on the Internet	28
Chapter 12: How to use removable media securely	30
Chapter 13: How to secure your mobile workforce	31
Chapter 14: How to buy online safely	32
Chapter 15: Education and Technology: A Winning Cyber Security Combination	34
The Value of Connexiom' Cyber Security Services	35
Learn more	36
Glossary	37
Resources	43

How to use this edition

The original guide's body content is retained. Jedi Notes add Star Wars examples and practical context. Clearly marked Security Updates clarify older recommendations without silently removing the original material. Historic statistics, product examples, and forecasts remain source material rather than current verified claims. Use your organization's current policies and IT/security guidance for operational decisions.

CONNEXIOM / FULL-CONTENT JEDI EDITION

About Connexiom

JEDI NOTE / Hello there. Meet your team of technology Jedis.

Connexiom helps businesses connect their people, systems, and spaces with practical IT and cybersecurity. This is the full guide: all 15 chapters, detailed examples, checklists, glossary, and original resources. Jedi Notes add galactic perspective without replacing the training.

Connexiom is an Information Technology (IT) Managed Services Provider (MSP) company focusing on serving the Small-Medium Business (SMB) market since 2022. With many years of expertise, we are dedicated to providing enterprise level experience, excellent customer service, and unmatched response time to our clients. Our goal is to implement the RIGHT technology for each client resulting in savings and success for their business. We are not just an IT company, but a partner that wants to earn your business each and every day.

CONNEXIOM / FULL-CONTENT JEDI EDITION

Are You Prepared for a Cyber Attack?

JEDI NOTE / Never tell me the odds. Show me the plan.

A smaller business is not an invisible Rebel base. Use these questions to find gaps in ownership, detection, response, and training. Question 2 is reverse-scored: being uncomfortable with a competitor obtaining client data is the sensible answer. The goal is to protect that information.

Can You Answer Yes to All of these Questions?

1. Do you currently have cyber security with 24x7x365 threat monitoring and management?
2. If your biggest competitor obtained all of your customers' information, would you be ok with that?
3. Do you have a plan and partner you could call if you came into work tomorrow and were unable to access all of your files because they were locked?
4. Do you have an incident response plan with clear roles and responsibilities for your team?

5. Are you meeting with employees on a regular basis to ensure your response plan is effective?
6. Are your employees receiving regular cybersecurity training?
7. Do you have effective password management policies in place in your business?

If you answered no to any of these questions, then it may be time to upgrade your cybersecurity strategy. Have you ever thought, “That will never happen to me” or “It’s a risk I’m willing to take.”? Small and medium sized businesses (SMBs) are the prime target for attackers because they tend to be easier targets. They’re often less secure and unprepared for attack. Think about burglars that go after houses where they know no one is home. With more cybercrime automation and the rise of hacking kits, the cost and time it takes to launch a successful attack have decreased, increasing the amount of cyber-attacks executed. 82 percent of SMBs say they’re not targets for attacks as they don’t have anything worth stealing. It doesn’t always seem like it, but every business has data worth stealing.

Did you know that the average cost per lost or stolen record is \$158? It may not seem like a lot, but this number grows quickly once these records are stolen by the hundreds.

Our team of security experts are here to support your business 24x7x365 to ensure that no matter what type of threat enters your network, we can help keep your business secure. Partner with Connexiom to protect against the expanding cyber threat landscape, and mitigate damages inflicted upon your business. Gain the expertise, technology and support you may be lacking, and grow your IT budget without growing your payroll.

CONNEXIOM / FULL-CONTENT JEDI EDITION

Introduction: The Need to Educate Employees on Cybersecurity

JEDI NOTE / The Jedi Academy is now in session.

A firewall cannot teach an employee to question a convincing request. Train people, practice realistic scenarios, and make reporting easy. Statistics reproduced from the original guide are historical source figures and forecasts, not independently verified current measurements.

When developing cybersecurity programs, many businesses focus on protecting their infrastructure perimeter and device endpoints. After all, that's where cybercriminals usually first gain access and wreak havoc on a company's digital access.

But it's also important to consider what happens when a threat bypasses perimeter defenses and targets an employee - in the form of a malicious email or text, or even a voicemail that might prompt an employee to respond with confidential company information. There's also the possibility of an offline attack from inside the office, where an employee or an office visitor might gain access to valuable data by quickly taking something carelessly left on a desk.

According to a recent Pricewaterhouse-Coopers survey, 86% of business executives expressed concern about cyber threats, including a lack of data security. In addition, 100% of IT professionals recently surveyed at an SMB said they could improve their cybersecurity systems. These numbers indicate that it's clear there's a pressing need for better cybersecurity. The issue is not going away anytime soon and it's only getting worse.

Stronger cybersecurity has become a global priority over the last few years as hackers penetrate the IT infrastructure of government and enterprises with increasing frequency and sophistication. According to a recent government report, How to Protect Your Networks from Ransomware, 4,000 ransomware attacks occurred per day in 2016. Furthermore, the annual cost of global cybercrime damages are estimated to cost \$10.5 trillion by 2027, according to a 2025 Cybercrime Report by Cybersecurity Ventures. Coupled with the

Internet of Things (IoT) and the explosive growth of mobile devices, the threat landscape and potential for data leaks is even more significant.

In this guide, we explore the need for employees to practice strict and secure cybersecurity habits - not only to thwart digital attacks, but also to prevent someone from simply walking by their desk (in the office or at home) and picking up a device or document that contains sensitive information. We also present the key steps business owners can take to educate their employees to help secure their company's data and intellectual property.

We can't stress enough the importance of security awareness training for internal employees. Educating them on what it takes to protect proprietary documents and data is critical. Any leaks - unintentional and intentional - could hurt the business in the form of information that assists a competitor, violates regulations, or harms the corporate image. Leaks can also hurt employees from the standpoint of personal information that might be exposed. Lastly, customers and business partners could be at risk, compromising the industry reputation of any business that does not properly protect confidential information. It only takes one incident to completely destroy any goodwill you established and built with your customer base.

CONNEXIOM / FULL-CONTENT JEDI EDITION

Chapter 1: Physical Security

Precautions

JEDI NOTE / These aren't the droids you're looking for.

That line is funny in a film. It is a poor visitor policy. Lock your screen, secure documents and devices, challenge unfamiliar visitors through the approved process, and keep the clean-desk checklist below in your team's training.

Keep a Clean Desk

It makes complete sense and sounds so simple, but keeping a clean desk is often overlooked when talking about data security. It's also the perfect place to start the discussion with employees.

Employees that keep a cluttered desk tend to leave USB drives and smartphones out in the open. They also often forget to physically secure their desktops and laptops so someone can't simply walk off with them.

A messy desk also makes it more difficult to realize something is missing such as a folder with hard copy print-outs of customer lists. In addition to increasing the likelihood of something being removed, a cluttered desk means that the discovery of any theft will likely be delayed - perhaps by days or even weeks if the employee is out of the office. Such delays make it more difficult to determine who the perpetrator is and where the stolen material might now be located.

Encouraging employees to maintain a neat desk pays off in two ways. In addition to making digital and paper assets more secure, employees with clean desks are more apt to be productive because they can quickly - and safely - access the tools and resources they need to do their jobs.

Common Messy Desk Mistakes to Avoid

The following list presents 11 "messy desk" mistakes employees are prone to commit and which could cause irreparable harm to the business, the employee, fellow employees, customers and business partners. These are all bad habits for which to educate employees to stop:

1. Leaving computer screens on without password protection: Anyone passing by has easy access to all the information on the device; be sure to lock down screen settings.
2. Placing documents on the desk that could contain sensitive information: It's best to keep them locked up in drawers and file cabinets.
3. Forgetting to shred documents before they go into the trash or recycling bin: Any document may contain sensitive information; it's best to shred everything rather than taking a risk.
4. Failing to close file cabinets: This makes it easy for someone to steal sensitive information and more difficult to realize a theft has occurred.
5. Setting mobile phones and USB drives out in the open: They likely contain sensitive business or personal information and are easy to pick up quickly without being caught in the act.
6. Neglecting to erase notes on whiteboards: They often display confidential information on products, new ideas and proprietary business processes.
7. Dropping backpacks out in the open: There's often at least one device or folder with sensitive information inside.
8. Writing user names and passwords on slips of paper or post-its: This is especially important given that user names and passwords are typically used to log in to more than one site.
9. Leaving behind a key to a locked drawer: This makes it easy to come back later - perhaps after hours when no one is around - and access confidential files.
10. Displaying calendars in the open or on the screen for all to see: Calendars often contain sensitive dates and/or information about customers, prospects and/or new products.
11. Leaving wallets and credit cards out on the desk: This is more likely to impact the employee, but wallets may also possess corporate credit cards and security badges.

In today's fast-paced world where employees are always on the go, it takes too much time to determine whether documents, USB drives, devices and other items contain sensitive information. The safe bet is to make sure everything is filed away and kept locked up or else properly destroyed.

CONNEXIOM / FULL-CONTENT JEDI EDITION

Chapter 2: Email Threats

JEDI NOTE / It's a trap! Even when it sounds like the Emperor.

A familiar name, urgent tone, or convincing voice does not prove identity. Verify payment changes, credentials, and remote-access requests through a known independent channel. Report suspicious messages with the company's approved tool; do not circulate live malicious attachments.

Social Engineering Inboxes and VoiceMail

Social engineering is non-technical, malicious activity that exploits human interactions to obtain information about internal processes, configuration and technical security policies in order to gain access to secure devices and networks. Such attacks are typically carried out when cybercriminals pose as credible, trusted authorities to convince their targets to grant access to sensitive data and high-security locations or networks.

An example of social engineering is a phone call or email where an employee receives a message that their computer is sending bad traffic to the Internet. To fix this issue, end users are asked to call or email a tech support hotline and prompted to give information that could very likely give the cybercriminal access to the company's network.

Phishing Email Compromises

One of the most common forms of social engineering is email phishing - an attempt to acquire sensitive information such as usernames, passwords and credit card data by masquerading as a trustworthy entity. Phishing is likely the #1 primary email threat employees need to focus on.

Such emails often spoof the company CEO, a customer or a business partner and do so in a sophisticated, subtle way so that the victim thinks they are responding to a legitimate request.

Among the reasons these scams succeed are the appearance of authority - staffers are used to carrying out CEO instructions quickly. That's why phishing can be so easy to fall victim to.

Four Common Phishing Techniques

The scope of phishing attacks is constantly expanding, but frequent attackers tend to utilize one of these four tactics:

- Embedding links into emails that redirect users to an unsecured website requesting sensitive information.

- Installing Trojans via a malicious email attachment or posing ads on a website that allow intruders to exploit loopholes and obtain sensitive information.
- Spoofing the sender address in an email to appear as a reputable source and requesting sensitive information.
- Attempting to obtain company information over the phone by impersonating a known company vendor or IT department.

Email Security Best Practices - Five Ways to Block Phishing Attacks

Employees should always be suspicious of potential phishing attacks, especially if they don't know the sender. Here are five best practices to follow to help make sure employees don't become helpless victims:

1. Don't reveal personal or financial information in an email - Make sure employees also know not to respond to email solicitations for this information. This includes clicking on links sent in such emails.
2. Check the security of websites - This is a key precaution to take before sending sensitive information over the Internet. <http> indicates the site has not applied any security measures while <https> means it has. Also consider if employees are practicing safe browsing habits. Sites that do not serve a legitimate business purpose are also more likely to contain harmful links.
3. Pay attention to website URLs - Not all emails or email links seem like phishing attacks, so employees may be lured into a false sense of security. Teach them that many malicious websites fool end users by mimicking legitimate websites. One way to sniff this out is to look at the URL (if it's not hidden behind non-descript text) to see if it looks legit. Employees may also be able to detect and evade the scheme by finding variations in spellings or a different domain (e.g., .com versus .net).
4. Verify suspicious email requests - Contact the company they're believed to be from directly. If an employee receives an email that looks odd from a well-known company, such as a bank, instruct them to reach out to the bank using means other than responding to the suspicious email address. It's best to contact the company using information provided on an account statement - NOT the information provided in the email.
5. Keep a clean machine - Utilizing the latest operating system, software and Web browser as well as antivirus and malware protection are the best defenses against viruses, malware and other online threats. It may be difficult for employees to do this, so the business should partner with a managed IT services provider like Connexiom who can also be a trusted advisor for all IT needs.

CONNEXIOM / FULL-CONTENT JEDI EDITION

Chapter 3: Username and Password Management

JEDI NOTE / The password is not “DeathStar123!”

Predictable substitutions do not create a strong secret. Use long, unique, randomly generated passwords or approved passkeys and enable MFA. Prefer phishing-resistant MFA where available. A password hash is a one-way derivation, not reversible encryption. See the Security Update below for the original rotation advice.

Low Security Account Credentials

Although it should be common sense, employees need to avoid the use of passwords that are easy for hackers to guess. Among the top ten worst passwords are those that use a series of numbers in numerical order, such as <123456>. The names of popular sports such as <football> and <baseball> are also on the list as are quirky passwords such as <qwerty> and even the word <password> itself.

Emphasis should also be placed on the importance of avoiding common usernames. In analysis conducted by the information security firm Rapid7, hackers most often prey upon these 10 usernames in particular:

• Username • administrator • Administrator • user1 • Admin • Alex • Pos • Demo • db2admin • Sql

How Attackers Exploit Weak Passwords to Obtain Access

While most websites don't store actual username passwords, they do store a password hash for each username. A password hash is a form of encryption, but cybercriminals can sometimes use the password hash to reverse engineer the password. When passwords are weak, it's easier to break the password hash.

Here is a list of common word mutations hackers use to identify passwords if they feel they already have a general idea of what the password might be:

- Capitalizing the first letter of a word
- Checking all combinations of upper/lowercase for words
- Inserting a number randomly in the word

- Placing numbers at the beginning and the end of words
- Putting the same pattern at both ends, such as <foobar>
- Replacing letters like <o> and <l> with numbers like <0> and <1>
- Punctuating the ends of words, such as adding an exclamation mark <!>
- Duplicating the first letter or all the letters in a word
- Combining two words together
- Adding punctuation or spaces between the words
- Inserting <@> in place of <a>

Educating end users on these tactics underscores the importance of creating long passwords (at least 12 characters) and applying multiple deviations, rather than something simple like just capitalizing the first letter.

Nine Tips to Strengthen Password Security

JEDI NOTE / SECURITY UPDATE / Keep the access code strong.

The original rotation recommendations follow for completeness. NIST guidance says not to require routine password changes without evidence of compromise. Use a long, unique password, a blocklist of weak/compromised choices, and appropriate MFA. Change a password promptly when compromise is suspected or confirmed. Use your organization's approved policy and password manager.

1. Change passwords at least every three months for non-administrative users and 45-60 days for admin accounts.
2. Use different passwords for each login credential.
3. Avoid generic accounts and shared passwords.
4. Conduct audits periodically to identify weak/duplicate passwords and change as necessary.
5. Pick challenging passwords that include a combination of letters (upper and lower case), numbers and special characters (e.g. <\$>, <%> and <&>).
6. Avoid personal information such as birth dates, pet names and sports.
7. Use passwords or passphrases of 12+ characters.
8. Use a Password Manager such as 1Password where users need just one master password.
9. Don't use a browser's auto-fill function for passwords.

An advanced and under-used password security tip to consider is two-factor authentication, which is a way for websites to double confirm an end user's identity. After the end user successfully logs in, they receive a text message with a passcode to then input in order to authenticate their ID.

This approach makes sure that end users not only know their passwords but also have access to their own phone. Two-factor authentication works well because cybercriminals rarely steal an end user's password and phone at the same time. Leading banks and financial institutions enable two-factor authentication by default, but if not, the service can often be turned on by asking the website to do so. More and more non-financial websites are now offering two-factor authentication as well.

CONNEXIOM / FULL-CONTENT JEDI EDITION

Chapter 4: Mobile Security

JEDI NOTE / Your pocket-sized astromech needs protection, too.

A phone can hold the keys to the whole Rebel base. Use supported devices, managed work apps, a strong screen lock, encryption, updates, and prompt loss reporting. Remote location or wiping depends on prior setup, device connectivity, authorization, and platform support; it is not guaranteed.

Mobile Threats Jeopardizing Company Data

Mobile security is increasingly becoming a big concern as more and more companies adopt Bring Your Own Device (BYOD) environments, which allow end users to connect to corporate networks through their own (often multiple) devices. Even in cases where a business does not offer BYOD, end users often find a way to log onto business networks on their own. With personal devices accessing corporate networks, businesses must now protect endpoint devices that are not completely under their control, which opens up the business to greater risk. Trying to gain control over personal devices also presents the challenge of making sure the company does not infringe on personal apps and information employees store on their own devices.

Mobile Device Security Challenges

- Lost, misplaced or stolen devices - remote wiping them quickly is key to protecting sensitive business and personal information.
- Mobile malware - hackers are now turning their attention to mobile devices and executing successful breaches through text messages. Android markets can be set up by anyone looking to sell malicious software to unsuspecting customers. Note: While mobile malware affects Androids more than iOS, a few exploits exist for Apple products as well.
- Unsecure third-party apps - if breached, they can serve as a gateway to other apps on a device and the device operating system, where security controls can be manipulated.
- Files with sensitive information accidentally emailed to an unauthorized party or posted online - once something is sent, it's out there forever.

Employees that utilize unsecured public Wi-Fi are another area of concern. Hackers in the vicinity of or on the same network can overtake a device without the end user even being aware, capturing sensitive data in transit. The end user can then become the victim of a man-in-the-middle attack, also referred to as hijacking. The hacker leverages the device so that it turns into an invasive device against other unsuspecting end users.

How Employees Can Secure Their Mobile Devices

Set a PIN or passcode: This is the first line of defense - if someone wants to access the device, they first need to break the code. This is not an easy task and can operate as a deterrent against theft. Some device manufacturers also provide the option to automatically wipe the device after a few unsuccessful attempts at the passcode or PIN. So even if a phone is stolen, information cannot be accessed.

Use remote locate tools: Several software solutions help locate lost or stolen devices through GPS and geofencing capabilities. Apple offers a service like this for mobile devices aptly named Find my iPhone. For Android users, the Android Device Manager offers these services, and Windows mobile users have this same option from the Windows Phone website. Similarly, many third-party applications are available in each of the app stores.

Keep devices clean: Phones are mini-computers, and just like “big” computers, they need to be cleaned up from time-to-time. Utilizing an antivirus and malware scanner is always a good idea. Malware can compromise information stored on mobile devices and has a snowball effect that continuously piles up until it slows down or stops the device.

Mobile Device Management (MDM) solutions help businesses and their employees apply these best practices by providing the ability to remotely wipe any devices that are lost or stolen. Such solutions also isolate personal apps from corporate apps in separate digital containers so that personal information remains private, and when an employee leaves the company, only their corporate apps and data are deleted while their personal apps and data are left intact.

By deploying an MDM platform, businesses can also enforce the use of passcodes to access devices, and they can apply geofencing capabilities that allow a lost device to be more easily located. End users can also be restricted to using only the corporate apps for which they have proper authorization. MDM also protects devices from jailbreaking and rooting - where hackers try to gain access to the operating system to open security holes or undermine the device’s built-in security measures.

CONNEXIOM / FULL-CONTENT JEDI EDITION

Chapter 5: Secure Website Browsing

JEDI NOTE / That's no moon. It's a lookalike website.

Branding, advertisements, and a padlock are not proof that a site is honest. HTTPS encrypts the connection; malicious sites can use it too. Use current browsers and TLS, verify the domain, and treat unsolicited downloads with suspicion. Older social-network statistics and examples below are retained from the source guide.

The Top Browser Threats

When end users venture out onto the Internet, it's easy to get tangled up in the vast web of threats lurking on many website pages. Some of them are readily apparent, but others are well hidden.

Malvertising - a form of malicious code that distributes malware through online advertising - can be hidden within an ad, embedded on a website page, or bundled with software downloads. This type of threat can be displayed on any website, even those considered the most trustworthy.

End users also need to beware of social media scams. Hackers have created a playground of virtual obstacles across all the major social media sites. According to an article in The

Huffington Post, some of the most common Facebook hacks and attacks include click-jacking, phishing schemes, fake pages, rogue applications and the infamous and persistent Koobface worm, which gives attackers control of the victim's machine while replicating the attack to everyone on their Facebook contact list.

X (formerly Twitter) isn't immune to security issues either. Since the microblogging site is both a social network and a search engine, it poses extra problems. According to CNET News, just 43% of X users could be classified as "true" users compared to the other 57%, which fell into a bucket of "questionable" users. Among the things to watch for on Twitter are direct messages that lead to phishing scams and shortened URLs that hide malicious intentions.

As for Web-based exploits, Internet websites are now the most commonly-used angles of attack, most often targeting software vulnerabilities or using exploits on the receiving client. This makes keeping up-to-date browsers paramount for all employees.

Website Browsing Best Practices for Employees

- Be conservative with online downloads.
- Beware antivirus scams.
- Interact only with well-known, reputable websites.
- Confirm each site is the genuine site and not a fraudulent site.
- Determine if the site utilizes SSL (Secure Sockets Layer), a security technology for establishing encrypted links between Web servers and browsers.
- Don't click links in emails - go to sites directly.
- Use social media best practices.

CONNEXIOM / FULL-CONTENT JEDI EDITION

Chapter 6: How to avoid Viruses, Trojans, Worms and Spyware

JEDI NOTE / A Trojan is not a helpful protocol droid.

Keep layered endpoint and email protection current, control unapproved software and devices, and patch supported systems. Backups need restore tests and protection from the incident affecting production. A green backup notification alone is not a successful recovery mission.

Use antivirus or endpoint security software

Install antivirus or endpoint security software on all your desktops and servers, and make sure to keep them up to date. New malware can spread extremely quickly, so have an infrastructure in place that can update all the computers in your organization seamlessly, frequently and on short notice.

To protect against email-borne viruses, spam and spyware, run email filtering software at your gateway.

And don't forget to protect laptop computers, desktop computers and mobile devices used by employees who telecommute.

Block file types that often carry malware

Block executable file types from being received by email or downloaded from the Internet. It is unlikely that your organization will ever need to receive these types of files from the outside world.

Subscribe to an email alert service

Consider adding a live malware information feed to your website or intranet so your users know about the very latest computer threats.

Use a firewall on all computers

Use a firewall to protect computers that are connected to a network. Many worms can enter even a closed network via USB drives, CDs and mobile devices. Laptops and telecommuters will also need firewall protection.

Stay up to date with software patches

We encourage using automatic (patch) updating, especially in the case of Windows computers. Patches often close loopholes that can make you vulnerable to malware threats.

Back up your data regularly

Make regular backups of important work and data, and check that the backups were successful. You should also find a safe place to store your backups, preferably off-site in case of fire. If your computer is infected with malware, you will be able to restore any lost programs and data. Any sensitive backup information should be encrypted and physically secured.

Implement device control

Prevent unauthorized devices from connecting to your computers. Unauthorized devices such as USB drives, music players and mobile phones can carry malware that will infect a computer when plugged in.

CONNEXIOM / FULL-CONTENT JEDI EDITION

Chapter 7: How to secure your data

JEDI NOTE / Protect the plans before they leave the Rebel base.

Encryption, approved sharing, access controls, and data-loss prevention work together. Encryption does not prevent deletion, every kind of data loss, or misuse by an authorized account. Use approved cloud services with managed identity, sharing, and recovery settings; cloud storage is not inherently unsecured.

Encrypt your computers, emails and other devices

By encrypting your data, you can make sure that only authorized users with the appropriate encryption key or password can access the information. With encryption you can keep your data secure at all times, even if it is stored on a laptop, CD or other device that is lost or stolen, or if it's contained in an intercepted email.

Use device and application control

Prevent users from accessing peer-to-peer file sharing and USB drives. These are common paths for data loss.

Only allow computers that comply with your security policy to access your network. This could include requirements for encryption, or device or application control technologies.

Block employee access to cloud-based mail services

Put controls in place to monitor or block employee use of cloud storage services such as Dropbox. These controls should include applying web-based URL filtering, application controls and data encryption. You can prohibit access and transfer of confidential information to largely unsecured cloud-based storage services.

Implement outbound content controls

Identify the sensitive data you want to control (e.g., any files containing the term "confidential" or credit card numbers) and then decide how these files can be used. For example, you may wish to present the user with a warning about potential data loss, or prevent distribution of the data by email, blogs or forums.

An encryption solution allows users to choose their preferred cloud storage services because the files are always encrypted and the keys are always your own. And because encryption takes place on the client before any data is synchronized, you have full control of the safety of your data.

User wireless encryption

Configure your office wireless networks to use strong encryption, such as that offered by WPA2. Encourage your employees to do the same on their home wireless networks.

CONNEXIOM / FULL-CONTENT JEDI EDITION

Chapter 8: How to avoid SPAM

JEDI NOTE / These aren't the offers you're looking for.

Spam is not a bargain from a friendly Jawa. Use managed filtering and the approved report/junk controls. Blocking remote images can reduce tracking. Modern, patched mail clients differ in preview behavior, so follow IT's settings rather than treating preview mode alone as the security boundary.

Use email filtering software at your email gateway

You should run email filtering software at the email gateway to protect your organization from spam as well as email-borne spyware, viruses and worms.

Never make a purchase from an unsolicited email

By making a purchase, you are funding future spam. Spammers may add your email address to lists to sell to other spammers, so that you receive even more junk email. Worse still, you could be the victim of a fraud. If you do not know the sender of an unsolicited email, delete it. Spam can contain malware that damages or compromises the computer when the email is opened.

Don't use the preview mode in your email viewer

Many spammers can track when a message is viewed, even if you don't click on the email. The preview setting effectively opens the email and lets spammers know that you receive their messages. When you check your email, try to decide whether a message is spam on the basis of the subject line only.

Don't overexpose your email address

How much online exposure you give your email address is the biggest factor in how much spam you receive. Here are some bad habits that expose your email address to spammers:

- Posting to mailing lists that are archived online
- Submitting your address to online services with questionable privacy practices
- Exposing your address publicly on social networks (Facebook, LinkedIn, etc.)
- Using an easily guessable address based on first name, last name and company
- Not keeping your work and personal email separate

- Use the bcc field if you email many people at once

The bcc or blind carbon copy field hides the list of recipients from other users. If you put the addresses in the To field, spammers may harvest them and add them to mailing lists.

Use one or two secondary email addresses

If you fill out web registration forms or surveys on sites from which you don't want further information, use a secondary email address. This protects your main address from spam.

Opt out of further information or offers

When you fill out forms on websites, look for the checkbox that lets you choose whether to accept further information or offers. Check or uncheck the box as appropriate.

CONNEXIOM / FULL-CONTENT JEDI EDITION

Chapter 9: How to avoid being Phished

JEDI NOTE / Admiral Ackbar had the right instinct.

Pause before opening an unexpected invoice, password-reset link, or “urgent” executive request. Attackers can write flawless messages, so grammar is not a reliable test. Verify independently, and report promptly if you clicked, shared information, or approved an unexpected MFA prompt.

Never respond to emails that request personal financial information!

You should be suspicious of any email that asks for your password or account information or includes links for that purpose. Banks and ecommerce companies do not usually send such emails.

Look for signs that an email is "phishy"

Some phishing emails are generic, using greetings like "Dear valued customer." They may also include alarming claims (e.g., your account numbers have been stolen), use suspiciously poor spelling or grammar and/or request that you take an action like clicking a link or sending personal information to an unknown address. Other phishing emails are more targeted and may be very believable. Look for unusual behavior, such as a blank or irrelevant attachment (which could have hidden malware), or a request to click a link that doesn't fit with the topic or sender of the message.

Visit bank websites by typing the address into the address bar

Don't follow links embedded in an unsolicited email. Phishers often use these to direct you to a bogus site. Instead, you should type the full address into the address bar in your browser.

Keep a regular check on your accounts

Regularly log in to your online accounts and check your statements. If you see any suspicious transactions, report them to your bank or credit card provider.

Make sure that the website you are visiting is secure

Check the web address in the address bar. If the website you are visiting is on a secure server, it should start with https:// ("s" stands for secure) rather than the usual http://. Also look for a small padlock icon on the browser's status bar. These signs tell you that the website is using encryption. However, even if a site is secure, there is no guarantee that it is safe because hackers can create websites that use encryption that are designed to steal personal information.

Be cautious with emails and personal data

Always conduct transactions safely. Don't let anyone know your PINs or passwords, do not write them down, and do not use the same password for all your online accounts. Don't open or reply to spam emails as this lets the sender know that your address is valid and can be used for future scams.

Keep your computer secure

Anti-spam software will prevent many phishing emails from reaching you. A firewall also helps to keep your personal information secure and block unauthorized communications. You should also run antivirus software to detect and disable malicious programs, such as spyware or backdoor Trojans, which may be included in phishing emails. Keep your Internet browser up-to-date with the latest security patches.

Always report suspicious activity

If you receive an email you suspect isn't genuine, forward it to the spoofed organization. Many companies have a dedicated email address for reporting such abuse.

CONNEXIOM / FULL-CONTENT JEDI EDITION

Chapter 10: How to choose secure passwords

JEDI NOTE / Size matters not? Password length disagrees.

Choose unique, long random passwords or randomly selected passphrases, store them in an approved password manager, and protect the manager itself. Familiar Star Wars quotes, character names, and examples printed in this guide are not suitable passwords.

Make your password as long as possible

The longer a password is, the harder it is to guess or to find by trying all possible combinations (i.e., a brute force attack). Passwords of 14 characters or more are vastly more difficult to crack.

Use different types of characters

Include numbers, punctuation marks, symbols, and uppercase and lowercase letters. On mobile devices that are not designed for easy special character input, consider using longer passwords with different characters.

Don't use dictionary words

Don't use words, names or place names that are usually found in dictionaries. Hackers can use a dictionary attack (i.e., trying all the words in the dictionary automatically) to crack these passwords.

Don't use personal information

Other people are likely to know information such as your birthday, the name of your partner or child, or your phone number, and they might guess that you have used them as a password.

Don't use your username

Don't use a password that is the same as your username or account number. Use passwords that are difficult to identify as you type them in. Make sure that you don't use repeated characters or keys close together on the keyboard.

Consider using a passphrase

A passphrase is a string of words, rather than a single word. Unlikely combinations of words can be hard to guess.

Use a password manager

Memorizing all of your passwords can be frustrating but more secure than writing it down. Reputable password management programs can help you choose unique passwords, encrypt them and store them securely on your computer. Examples include 1Password.

Use different passwords for each account

If a hacker cracks one of your passwords, at least only one account has been compromised.

Don't tell anyone else your password

If you receive a request to confirm your password, even if it appears to be from a trustworthy institution or someone within your organization, you should never disclose your password (see Phishing emails).

Don't use your password on a public computer

Don't enter your password on a publicly available computer (e.g., in a hotel or Internet café). Such computers may not be secure and may have keystroke loggers installed.

Change your passwords regularly

JEDI NOTE / SECURITY UPDATE / Keep the access code strong.

The original rotation recommendations follow for completeness. NIST guidance says not to require routine password changes without evidence of compromise. Use a long, unique password, a blocklist of weak/compromised choices, and appropriate MFA. Change a password promptly when compromise is suspected or confirmed. Use your organization's approved policy and password manager.

The shorter or simpler your password is, the more often you should replace it.

CONNEXIOM / FULL-CONTENT JEDI EDITION

Chapter 11: How to be safe on the Internet

JEDI NOTE / Stay on target. Keep the fleet patched.

Use approved tools, supported software, appropriate filtering, and layered protection. A router or firewall does not make a malicious page safe. When a pop-up announces a crisis and demands a download, contact your real IT team through a known channel.

Keep up-to-date with security patches

Hackers frequently exploit vulnerabilities in operating systems and programs in an attempt to infect computers. Be aware of security updates for your computer's operating system, browser, plugins and other code that could be the target of hackers. If you can, set up your computer to automatically download security patches.

Use firewalls

A network firewall is installed at your organization's boundary and admits only authorized types of traffic. A client firewall is installed on each computer on your network, and also allows only authorized traffic, blocking hackers and Internet worms. In addition, it prevents the computer from communicating with the Internet via unauthorized programs.

Don't follow links in unexpected emails

Links in unexpected emails can take you to bogus websites, where any confidential information you enter, such as account numbers and passwords, can be stolen and misused.

In addition, hackers often try to direct you to malicious webpages by spamming out links via email.

Use different passwords for every site

You should use a different password for each site where you have a user account. That way, if a password is compromised, only one account will be affected. In addition, make sure that your passwords are hard to guess and never use a dictionary word as your password.

Consider blocking access to certain websites or types of web content

In a company environment, you may want to prevent users from accessing sites that are inappropriate for workplace use, or that may pose a security threat (e.g., by installing spyware on computers). You can do this with web filtering software or a hardware appliance. Even if users are allowed to visit websites, you should make sure that all webpages they visit are scanned for security threats.

Scan email for malware and spam

Anti-spam programs can detect unwanted email and prevent it from reaching users' inboxes, as well as scan for malware contained within the email.

Don't click on pop-up messages

If you see unsolicited pop-ups, such as a message warning that a computer is infected and offering virus removal, don't follow links or click to accept software downloads. Doing so could result in you downloading malicious code such as fake antivirus software.

Use routers

You can use a router to limit connections between the Internet and specific computers. Many routers also incorporate a network firewall.

CONNEXIOM / FULL-CONTENT JEDI EDITION

Chapter 12: How to use removable media securely

JEDI NOTE / An unknown USB drive is not a gift from the Rebellion.

Do not plug in found media to see what is on it. Use approved devices, encryption, and transfer rules; let IT evaluate unfamiliar storage. Encryption limits unauthorized reading when implemented correctly, but does not stop loss, destruction, or every malware risk.

Identify device types

Computers interact with a growing variety of removable media including USB drives, MP3 players and smartphones. Having visibility of what removable media is attempting to connect to your network can help you set appropriate restrictions or permissions.

Implement device control

Controlling the type of removable media that is permitted and what data is allowed to be exchanged is a vital component of network security. Choose solutions that can set permissions (or restrictions) for individual devices as well as entire classes of devices.

Encrypt your data

Data encryption prevents the loss of data. This is particularly useful for removable media that can be easily misplaced or stolen because the data cannot be viewed or copied by unauthorized third parties.

CONNEXIOM / FULL-CONTENT JEDI EDITION

Chapter 13: How to secure your mobile workforce

JEDI NOTE / Protect the crew beyond the home base.

Remote staff need the same ownership, patching, access controls, reporting, and recovery planning as office staff. Use approved remote access and MFA. A VPN protects a connection; it does not make an infected device or fraudulent website trustworthy.

Smartphones are standard business tools storing sensitive business information and enabling email on the move. This makes them vulnerable to attack from malware authors seeking out new ways to defraud users and steal confidential business data.

While mobile viruses and spyware remain a relatively small problem compared with the much larger amount of malware targeting Windows computers, the risks to business reputation, communication and continuity are becoming more serious. Risks include data theft, disruption of mobile phone networks and the hijacking of phones to send unauthorized revenue-generating SMS messages.

Mobile devices can be infected in many ways including email, MMS, external memory cards, PC synchronization and even via Bluetooth.

Make sure your security policy includes a strategy for mobile devices, covering:

- Threat management - identification and removal of viruses, spyware and spam
- Device access control and management enforcing a password policy and application management
- Data protection - encryption of sensitive data on devices and remote data deletion
- Network access control - controlling VPN connections across public networks, validation of devices when they connect to the corporate network

CONNEXIOM / FULL-CONTENT JEDI EDITION

Chapter 14: How to buy online safely

JEDI NOTE / Watto's deal may have a catch. Read the terms.

Verify the merchant, domain, payment route, return policy, and required information. Use approved company payment methods and independently confirm changed bank details. Keep receipts and review statements. Neither a familiar brand nor HTTPS guarantees a trustworthy transaction.

Can you trust your common sense and intuition?

Unfortunately, it isn't practical for users to determine if a website is safe or not with the naked eye.

Although invisible to the visiting online customer, hackers often target improperly secured legitimate websites. Being a large, well-established company is no guarantee that the site is safe.

Purchasing from a secure computer or device running the latest antivirus software, firewalls and security patches will significantly decrease your chances of becoming a victim. Never follow links from unsolicited online communications, such as email messages, social media posts, or instant messages. Spammers and hackers use social engineering techniques as lures to fraudulent or infected websites.

Only part with sensitive information like your personal or financial details when you are fully satisfied with the legitimacy of the company.

Familiarize yourself with the Terms of Use and the Data Protection Policy

Read the fine print. Terms can sometimes detail hidden and unexpected costs or obligations.

Only purchase through websites using encryption

URLs that start with https:// rather than http:// (the "s" stands for secure) are encrypting information during transfer. Another indicator of a website using encryption is a small padlock icon displayed in the Internet browser.

However, there is no guarantee that these sites are safe, as hackers can create websites that use encryption but are designed to steal personal information.

Provide the minimum amount of personal information

Leave optional fields blank: Middle name, date of birth, mobile phone number, hobbies. Many website operators request optional information alongside required information to process a business transaction. Compulsory fields are often identifiable by an asterisk.

Never share your password

Even if someone else is making the purchase for you, you should enter the password yourself and never share it with others.

To stop subsequent users from accessing your account without authorization, never select the "remember my password" option on a shared computer.

Buy local where possible

When the seller is based in a different country, it can be much more difficult and expensive to resolve any issues and to enforce consumer rights legislation.

Check your bank statements

Check your bank account transactions regularly, particularly after making purchases over the Internet, to be sure that all payments are legitimate. If you discover payments that you cannot identify, inform your bank immediately.

Keep your order confirmations and receipts

Always retain important information relating to a purchase in either printed or electronic format. This information will be very useful in resolving any issues relating to the purchase.

CONNEXIOM / FULL-CONTENT JEDI EDITION

Chapter 15: Education and Technology: A Winning Cyber Security Combination

JEDI NOTE / Do. Or do not. Train the crew.

Awareness and technology reinforce each other. Practice reporting and response rather than relying on one annual presentation. Connexiom can help connect employee habits, technical controls, and business ownership into a workable security routine.

As your business begins the journey to enhance its cybersecurity posture, it all starts with educating your employees. The tips provided within this guide along with some basic common sense can go a long way in making sure sensitive information does not fall into the wrong hands.

This is where Connexiom can assist. We eliminate the need for your business to keep up on the latest antivirus, anti-malware and alert technologies. You also don't need to expend the necessary resource time to deploy and manage such solutions, which often fall beyond the bandwidth and expertise of internal teams.

Succeeding in applying the necessary cybersecurity measures is paramount to your long-term business success. In today's world of advanced hackers, who revel in breaching corporate networks, confidential information will always be at risk. Businesses must take the necessary steps to protect their intellectual property, their confidential information and their reputations while also safeguarding their employees, customers and business partners.

CONNEXIOM / FULL-CONTENT JEDI EDITION

The Value of Connexiom' Cyber Security Services

JEDI NOTE / A Jedi Council for your business defenses.

The original service examples are retained below. Actual coverage, monitoring hours, tools, responsibilities, response commitments, exclusions, and project scope belong in your written agreement. No tool or service can guarantee that every attack will be prevented.

Seems like a lot of information and a lot of action items, doesn't it? That's why partnering with Connexiom will bolster your cybersecurity defenses. This is especially true when it comes to end user error. All the tools and solutions in the world won't protect your business from every attack. Human error is still highly dangerous, and many employees grow complacent at some point as they fail to follow best practices.

We offer managed services and security for your devices which can be very helpful in deploying the right protection for local and remote devices. We bundle the right solutions to keep your data safe.

Partnering with Connexiom makes sense, because we serve as your armed guardians for proactively preventing security leaks that employees might cause and mitigating damage when a leak occurs.

Here's a quick view of the benefits of our managed cyber security services can provide:

- Keep employee devices updated with the latest endpoint protection.
- Monitoring for threats including zero-day threats through typical outlets but also dark web monitoring
- Ensuring installation of updates to programs and applications when new versions and fixes become available.
- Patching for operating system when first available on a regular schedule.
- Password management to help keep user's login credentials safe.
- Cloud based and internal threat scanning and monitoring.
- Advanced email protection and backups.
- Offers guidance on how to mitigate any security program risks.

- End user training to keep your employees informed on the latest threats and techniques used by cyber criminals.
- Provide policies & procedures on how employees should handle a company's data.

There are too many threats to name that can do serious harm to your business and its information, so we bundle best in class tools for complete management which are utilized by our highly trained professionals who are always armed and ready to defend your business.

CONNEXIOM / FULL-CONTENT JEDI EDITION

Learn more

JEDI NOTE / Help me, Connexiom. My security needs a plan.

Bring one concern to a virtual Technology Risk & Opportunity Review. We will help identify a sensible next move. No hologram required: (770) 580-0440 or Solutions@connexiom.com. Book at calendly.com/connexiom-jdavis/30min.

Connexiom wants to be your long-term partner in business, not just another service provider. Our team is composed of some of the most passionate and dedicated individuals in the industry. We love what we do, and it shows in the exceptional quality of our work. We're here to help our clients see tangible results, not just talk about it!

Let's Start Planning Your IT Cybersecurity Journey:

- Contact Connexiom to analyze your current security posture.
- Get a customized IT security strategy built just for you.

Contact us by visiting us at www.connexiom.com, calling us at (770) 580-0440 or emailing us at Solutions@connexiom.com.

We look forward to securing your business!

CONNEXIOM / FULL-CONTENT JEDI EDITION

Glossary

JEDI NOTE / Translate the transmission.

Keep the full glossary handy for team discussions. Security Update: a zero-day vulnerability is one without an available fix or otherwise unknown to relevant defenders; exploitation need not occur on the exact day it is discovered. Ransomware can also involve theft and extortion without encryption.

Application whitelisting

A security solution that allows organizations to specify what software is allowed to run on their systems, in order to prevent any non whitelisted processes or applications from running.

Asset inventory

A list of all IT hardware and devices an entity owns, operates or manages. Such lists are typically used to assess the data being held and security measures in place on all devices.

Cryptojacking

Cyber criminals compromise a user's computer or device and use it to mine cryptocurrencies, such as Bitcoin.

Custom threat intelligence

The collection and analysis of data from open source intelligence (OSINT) and dark web sources to provide organizations with intelligence on cyber threats and cyber threat actors pertinent to them.

Database encryption

Where sensitive data is encrypted while it is stored in databases. If implemented correctly, this can stop malicious actors from being able to read sensitive data if they gain access to a database.

Data loss prevention

Software that can identify if sensitive data is being exfiltrated from a network or computer system.

Denial of service

An attacker sends high volumes of connection requests to a server, resulting in a crash.

DDoS mitigation

A DDoS attack aims to disrupt the normal traffic of a targeted server, service, or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic. DDoS attacks achieve effectiveness by utilizing multiple compromised computer systems as sources of attack traffic.

DMARC

An internet protocol used to combat email spoofing - a technique used by hackers in phishing campaigns.

DNS filtering

A specific technique to block access to known bad IP addresses by users on your network.

DNS Tunnelling

A sophisticated attack vector that is designed to provide attackers with persistent access to a given target. Since many organizations fail to monitor DNS traffic for malicious activity, attackers can insert malware into DNS queries (DNS requests sent from the client to the server). The malware is used to create a persistent communication channel that most firewalls are unable to detect.

Drive-by Attack

A 'drive-by-download' attack is where an unsuspecting victim visits a website which in turn infects their device with malware. The website in question could be one that is directly controlled by the attacker, or one that has been compromised. In some cases, malware is served in content such as banners and advertisements. These days exploit kits are available which allow novice hackers to easily set up malicious websites or distribute malicious content through other means.

Email filtering

Software used to scan an organization's inbound and outbound email messages and place them into different categories, with the aim of filtering out spam and other malicious content.

Employee awareness

Training programs designed to increase employees' security awareness. For example, programs can focus on how to identify potential phishing emails.

Endpoint detection and response (EDR)

A software tool that works by monitoring and collecting data from endpoints and recording the information in a central database where further analysis, detection, investigation, reporting and alerting take place.

Endpoint protection

Software installed on individual computers (endpoints) that uses behavioral and signature based analysis to identify and stop malware infections.

Incident response plan

Action plans for dealing with cyber incidents to help guide an organization's decision-making process and return it to a normal operating state as quickly as possible.

Intrusion detection system (IDS)

An Intrusion Detection System (IDS) is a device or software application that monitors a network or systems for malicious activity or policy violations. Any detected activity or violation is typically reported either to an administrator or collected centrally using a security information and event management (SIEM) system.

Malware

Malware is any software intentionally designed to cause damage to a computer, server, client, or computer network. Examples include viruses, worms, Trojan horses, and ransomware. Malware exploits vulnerabilities to achieve its malicious goals.

Managed Service Provider (or MSP)

A third party organization that provides a range of IT services, including networking, infrastructure and IT security, as well as technical support and IT administration.

Mobile device encryption

Encryption involves scrambling data using cryptographic techniques so that it can only be read by someone with a special key. When encryption is enabled, a device's hard drive will be encrypted while the device is locked, with the user's passcode or password acting as the special key.

Multi-factor authentication

Where a user authenticates themselves through two different means when remotely logging into a computer system or web based service. Typically a password and a passcode generated by a physical token device or software are used as the two factors.

Network monitoring

A system, utilizing software, hardware or a combination of the two, that constantly monitors an organization's network for performance and security issues.

Next-generation firewalls

Software or hardware solutions that combines traditional firewall technology with additional functionality, such as encrypted traffic inspection, intrusion prevention systems and anti-virus.

Penetration tests

Authorized simulated attacks against an organization to test its cyber security defenses. May also be referred to as ethical hacking or red team exercises.

Perimeter firewalls

Hardware solutions used to control and monitor network traffic between two points according to predefined parameters.

Phishing

Phishing is a cyber attack that uses disguised email as a weapon. The goal is to trick the email recipient into believing that the message is something they want or need - a request from their bank, for instance, or a note from someone in their company - and to click a link or download an attachment.

Ransomware

An attacker obtains unauthorized access, encrypting the system (locking files and data) and asking for a financial sum of money before the computer is decrypted and operational.

Security info & event management (SIEM)

System used to aggregate, correlate and analyze network security information - including messages, logs and alerts - generated by different security solutions across a network.

Security Operations Centre (SOC)

A facility that houses an information security team responsible for monitoring and analyzing an organization's security posture on an ongoing basis. The SOC team's goal is to detect, analyze and respond to cybersecurity incidents using a combination of technology solutions and a strong set of processes. SOC's can be internal and run by the organization themselves or outsourced to a third party.

Social Engineering

Social engineering is the art of manipulating people so they give up confidential information. The types of information these criminals are seeking can vary, but when individuals are targeted the criminals are usually trying to trick you into giving them your passwords or bank information, or access your computer to secretly install malicious software.

Threat Intelligence

Threat intelligence, or cyber threat intelligence (CTI), is information an organization uses to understand the threats that have, will, or are currently targeting the organization. This information is used to prepare, prevent, and identify cyber threats looking to take advantage of valuable resources.

Two-Factor Authentication (2FA)

Two-factor authentication is a security process in which users provide two different authentication factors to verify themselves. This method is used to protect both the user's credentials and the resources the user can access, adding an extra layer of security.

Virtual private network (VPN)

A VPN is an encrypted connection over the internet from a device to a network. The encrypted connection helps ensure that sensitive data is safely transmitted. Most commonly used to provide a secure remote connection to an organization's network.

Vulnerability scans

Automated tests designed to probe computer systems or networks for the presence of known vulnerabilities that would allow malicious actors to gain access to a system.

Web application firewall

Protects web facing servers and the applications they run from intrusion or malicious use by inspecting and blocking harmful requests and malicious internet traffic.

Web content filtering

The filtering of certain web pages or web services that are deemed to pose a potential security threat to an organization. For example, known malicious websites are typically blocked through some form of web content filtering.

Written Information Security Program (WISP)

A Written Information Security Program (WISP) is a formal document that outlines an organization's approach to protecting its sensitive data and information systems.

Zero-day exploit

A zero-day exploit is a cyber attack that occurs on the same day a weakness is discovered in software. At that point, it's exploited before a fix becomes available from its creator. Zero- day refers to the fact that the developers have "zero days" to fix the problem that has just been exposed and perhaps already exploited.

CONNEXIOM / FULL-CONTENT JEDI EDITION

Resources

JEDI NOTE / The Jedi Archives: further training.

The original resource descriptions are retained. Additional current technical references: NIST Digital Identity Guidelines, pages.nist.gov/800-63-4/sp800-63b.html; CISA phishing-resistant MFA guidance, cisa.gov/audiences/small-and-medium-businesses/secure-your-business/require-multifactor-authentication. Follow your organization's approved policies and incident process.

- Framework for CyberSecurity - The NICE Workforce Framework for Cybersecurity (NICE Framework) (NIST Special Publication 800-181, revision 1) provides a set of building blocks for describing the tasks, knowledge, and skills that are needed to perform cybersecurity work performed by individuals and teams. Through these building blocks, the NICE Framework enables organizations to develop their workforces to perform cybersecurity work, and it helps learners to explore cybersecurity work and to engage in appropriate learning activities to develop their knowledge and skills.
- CyberSecurity 101 Video - NOVA Labs is a free digital platform that engages teens and lifelong learners in games and interactives that foster authentic scientific exploration
- Stay Safe Online - The National Cyber Security Alliance seeks to create a culture of cyber security and safety awareness by providing knowledge and tools to prevent cyber crime and attacks.
- FTC Consumer Advice - Practical tips from the federal government and the technology community to help people be on guard against Internet fraud, secure their computers, and protect their privacy.
- Cybersecurity Infrastructure & Security Agency - CISA is the operational lead for federal cybersecurity and the national coordinator for critical infrastructure security and resilience. We are designed for collaboration and partnership. Learn about our layered mission to reduce risk to the nation's cyber and physical infrastructure.
- FTC.gov/idtheft - The Federal Trade Commission's website has information to help people deter, detect, and defend against identity theft.
- ConnectSafely.org - ConnectSafely is for parents, teens, educators, and advocates for learning about safe, civil use of Web 2.0 together.
- Net Family News - NetFamilyNews.org's aim is to document developments at the intersection of youth and digital tech and media. It is now truly a blog and thus commentary more than reporting. In addition to Anne's writing, she does consulting on youth safety, literacy and

citizenship for social media platforms. For over a decade she has served as an online safety adviser as well.

- iKeepSafe.org - iKeepSafe educational resources teach children of all ages-in a fun, age appropriate way-the basic rules of Internet safety, ethics, and the healthy use of connected technologies.
- NetSmartz.org - The NetSmartz Workshop is an interactive, educational safety resource from the National Center for Missing & Exploited Children.

JEDI NOTE / May the Power to Connect and Control be with you.

Put the guide to work: choose one chapter for your next team discussion, practice a reporting scenario, and agree on who owns the next improvement. Book a virtual conversation with Connexiom at calendly.com/connexiom-jdavis/30min.