Does something seem "phishy" to you?

Millions of people are targets of phishing scams each day. Cyber criminals use a variety of tricks to disguise themselves as legitimate companies, your colleagues, and people you would normally trust. Make sure you know who you are really communicating with and be careful of suspicious links.

October is National Cyber Security Awareness Month. For more information and tips to stay safe online, visit: **https://www.dhs.gov/ncsam**

Homeland Security

National Cyber Security Awareness Month

CyberAware

How to Spot a Phishing Scam

Cyber crime is a critical threat with social engineering attacks becoming more sophisticated, realistic, and difficult to recognize. Phishing attacks are one of the most common forms of cyber crime. What does a phishing email look like? Review the example below for characteristics of a phishing scam disguised to look like a legitimate email.

Generic subject line

Legitimate emails usually have detailed subject lines. A vague subject line can be a key indicator of a phishing scam.

Suspicious URL

Hover over links included in emails to see the actual destination of the URL.

Improper use of copyright

Watch for improper use of copyright information. This is used to make the phishing email look official.

From: Webmail Master Security (webmastersecurity@webmail.com)

Subject: Urgent Email

Dear Webmail User,

You are required to authenticate your account below to continue sending and receive messages. We strongly advice you to upgrade now to protect your web/Domain and avoid termination. Follow link to verify your email address immediately:
www.security.webmail.com.

Failure to update might process your account as inactive, and you may experience termination of services or undue errors. Please comply with new server requirements and read through the attached privacy policy.

Wondering why you go this email?

This email was sent automatically during routine security checks. We are trying to protect your account so you can continue using services uninterrupted.

Thanks,
Webmail Master
©2017 Webmail Domain

Bad grammar/spelling

Phishing emails often contain misspelled words and bad grammar. This is a sign that the email did not come from a professional organization or a real person you may know.

Unnecessary urgency

Use your intuition and if something 'feels' wrong, consider calling the organization or office directly to validate the email.

Types of Social Engineering

Phishing:

Online communications or emails designed to lure individuals into providing sensitive information.

Tip: When in doubt, throw it out. If an email looks suspicious, contact the organization/individual directly to validate the legitimacy of the email. You can also report the email to your email provider's IT Security department.

Ransomware:

A type of malware that prevents or limits users from accessing their system or select files, unless a ransom is paid to restore access.

Tip: Be proactive and protect against data loss by backing up your files and keeping them safe on a physical, external storage device.

Identity Theft:

An act of wrongfully obtaining and using another person's information that involves fraud or deception.

Tip: Be diligent before posting personal information online and think carefully before sharing information through apps and websites.

For more information and tips to stay safe online throughout the year, visit: https://www.dhs.gov/ncsam

Homeland Security

National Cyber Security Awareness Month

CyberAware

Internet Security

ALARM

Use of alarm systems in Sensitive Compartmented Information Facilities to ensure non-cleared personnel are under constant oversight to prevent unauthorized access to classified information

CRACKING

When an individual with extensive computer knowledge purposely breaches, bypasses internet security, or gains access to software without paying royalties

SCANNING

Communicating with a web application in order to identify potential security vulnerabilities in the web application and architectural weaknesses

INSIDER THREAT

A malicious threat to an organization that comes from the likelihood, risk, or potential that an insider will use their authorized access, wittingly or unwittingly, to do harm to the national security of the United States.

HACKER

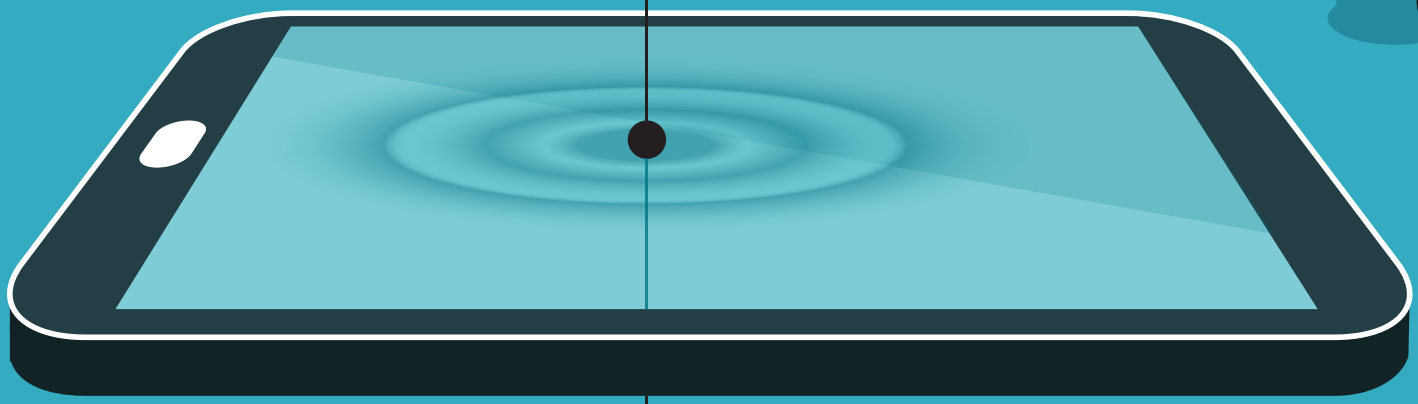
A person who secretly gets access to a computer system in order to get and/or tamper information, cause damage, or otherwise illegaly comporises an electronic service or system

VIRUS

A malware program that, when executed, replicates by inserting copies of itself (possibly modified) into other computer programs, data files, or the boot sector of the hard drive; when this replication succeeds, the affected areas are then said to be "infected"

DON'T GET REELED IN.

Phishing is a scam by which an email user is duped into revealing personal or confidential information that the scammer can use illicitly or fraudulently.



PHISHING PREVENTION 101

Secure yourself from fraud and phishing attempts by:

- Turning off the option to automatically download attachments
- Saving and scanning any attachments before opening them
- Before providing any kind of information, call and verify with the source that they are indeed the ones who sent the email or message

CDSE

For more information on phishing visit:

http://www.cdse.edu/toolkits/cybersecurity

BE CAREFUL

WHAT YOU POST ONLINE.

DON'T BECOME AN EASY TARGET.

Internet-based social networking sites have created a revolution in social connectivity. However, con artists, criminals, and other dishonest actors are exploiting this capability for nefarious purposes.

Preventive Measures Include:

- Do not store any information you want to protect on any device that connects to the Internet.
- Always use high security settings on social networking sites, and be very limited in the personal information you share. Monitor what others are posting about you on their online discussions.
- Use anti-virus and firewall software. Keep them and your browser, and operating systems patched and updated.
- Change your passwords periodically, and do not reuse old passwords. Do not use the same password for more than one system or service.
- Do not post anything that might embarrass you later, or that you don't want strangers to know.
- Verify those you correspond with. It is easy for people to fake identities over the Internet.

Center for Development of Security Excellence
CDSE

For more information on Social Networking Cybersecurity visit http://www.cdse.edu/toolkits/cybersecurity/socialmedia.html

THIS PAGE, HOW TO USE EMAIL SECURELY, IS OFFERED BY
COMMONWEALTH OF MASSACHUSETTS
Executive Office of Technology Services and Security
https://www.mass.gov/guides/how-to-use-email-securely#-general-email-security-reminders-

How to use email securely

This guide page provides a checklist of cyber security best practices for email use, including instructions on how to identify and respond to social engineering and phishing attempts.

General Email security reminders

- Do not use email for sensitive information
- Use caution when opening attachments - see the following section for more details
- Do not forward your work email to a personal email account
- Limit the amount of information in "Out of Office" messages and only send to internal users or users in your personal address book if possible
- Be sure to lock your computer screen when you walk away from your desktop or laptop computer
- Set your mobile device to lock and require a PIN
- Make sure your personal desktop and laptop computers at home are up to date with the latest security patches and anti-virus software

How to identify and respond to social engineering and phishing attempts

Social engineering is the art of obtaining confidential information from individuals through manipulative and deceptive means by mail, email (also known as phishing), or over the phone.

How can you identify a social engineering attempt via email?
There are several elements commonly found in most email-based social engineering/phishing attacks. Here are some red flags to watch out for:

Appearance
- Grammatical errors or misspellings
- Low quality or disorganized graphics or logos
- A generic greeting is used instead of your name

Sender's Identity
- Sender's name does not match email address
- Sender's email domain does not match the company the party claims to represent

Message / Tone
- Request includes opening an attachment, clicking a link, or providing sensitive information
- Urgency or warning of consequences if you do not respond

As hackers have become more sophisticated, their phishing emails have started to look more professional. Vigilance is crucial. If you have any doubts about an email, check with the help desk before responding or clicking on a link.

How should you respond if you encounter suspicious activity?

- Do not respond to emails or text messages asking for confidential or personal information.
- Do not open attachments or click on links within suspicious emails from an unknown individual.
- Attackers can target you at work through your personal accounts (like Gmail); follow the same care for all your accounts.
- Limit details disclosed in "out of office" messages.

ONLINE CYBERSECURITY ADVICE

for all digital citizens

The internet is a shared resource, and securing it is

Our Shared Global Responsibility.

LOCK DOWN YOUR LOGIN

Your usernames and passwords are not enough to protect key accounts like email, banking and social media. Strengthen online accounts and use strong authentication tools – like biometrics, security keys or a unique, one-time code through an app on your mobile device – whenever offered.

KEEP A CLEAN MACHINE

Keep all software on internet-connected devices – including personal computers, smartphones and tablets – current to reduce risk of infection from ransomware and malware.

WHEN IN DOUBT, THROW IT OUT

Links in email, tweets, posts and online advertising are often how cybercriminals try to compromise your information. If it looks suspicious, even if you know the source, it's best to delete or, if appropriate, mark it as junk.

BACK IT UP

Protect your valuable work, music, photos and other digital information by making an electronic copy and storing it safely. If you have a copy of your data and your device falls victim to ransomware or other cyber threats, you will be able to restore the data from a backup.

OWN YOUR ONLINE PRESENCE

Set the privacy and security settings on websites to your comfort level for information sharing. It is OK to limit how and with whom you share information.

SHARE WITH CARE

Think before posting about yourself and others online. Consider what a post reveals, who might see it and how it might affect you or others.

PERSONAL INFORMATION IS LIKE MONEY. VALUE IT. PROTECT IT.

Information about you, such as purchase history or location, has value – just like money. Be thoughtful about who gets that information and how it is collected by apps, websites and all connected devices.

STOP | THINK | CONNECT™

STOPTHINKCONNECT.ORG

@STOPTHNKCONNECT **STOPTHINKCONNECT**

STOP | THINK | CONNECT™

BASIC TIPS AND ADVICE

KEEP A CLEAN MACHINE

- KEEP SECURITY SOFTWARE CURRENT: Having the latest security software, web browser and operating system is the best defense against viruses, malware and other online threats.
- AUTOMATE SOFTWARE UPDATES: Many software programs will automatically connect and update to defend against known risks. Turn on automatic updates if that's an available option.
- PROTECT ALL DEVICES THAT CONNECT TO THE INTERNET: Along with computers, smartphones, gaming systems and other web-enabled devices also need protection from viruses and malware.
- PLUG & SCAN: USBs and other external devices can be infected by viruses and malware. Use your security software to scan them.

PROTECT YOUR PERSONAL INFORMATION

- LOCK DOWN YOUR LOGIN: Fortify your online accounts by enabling the strongest authentication tools available, such as biometrics, security keys or a unique one-time code through an app on your mobile device. Your usernames and passwords are not enough to protect key accounts like email, banking and social media.
- MAKE YOUR PASSWORD A SENTENCE: A strong password is a sentence that is at least 12 characters long. Focus on positive sentences or phrases that you like to think about and are easy to remember (for example, "I love country music."). On many sites, you can even use spaces!
- UNIQUE ACCOUNT, UNIQUE PASSWORD: Separate passwords for every account helps to thwart cybercriminals.
- WRITE IT DOWN AND KEEP IT SAFE: Having separate passwords for every account helps to thwart cybercriminals. At a minimum, separate your work and personal accounts and make sure that your critical accounts have the strongest passwords.

CONNECT WITH CARE

- WHEN IN DOUBT THROW IT OUT: Links in emails, social media posts and online advertising are often how cybercriminals try to steal your personal information. Even if you know the source, if something looks suspicious, delete it.
- GET SAVVY ABOUT WI-FI HOTSPOTS: Limit the type of business you conduct and adjust the security settings on your device to limit who can access your machine.
- PROTECT YOUR $$: When banking and shopping, check to be sure the site is security enabled. Look for web addresses with "https://" or "shttp://," which means the site takes extra measures to help secure your information. "Http://" is not secure.

STOP | THINK | CONNECT™

TIPS AND ADVICE

BE WEB WISE

- STAY CURRENT: Keep pace with new ways to stay safe online: Check trusted websites for the latest information, and share with friends, family, and colleagues and encourage them to be web wise.
- THINK BEFORE YOU ACT: Be wary of communications that implore you to act immediately, offer something that sounds too good to be true or ask for personal information.
- BACK IT UP: Protect your valuable work, music, photos and other digital information by making an electronic copy and storing it safely.

BE A GOOD ONLINE CITIZEN

- SAFER FOR ME, MORE SECURE FOR ALL: What you do online has the potential to affect everyone – at home, at work and around the world. Practicing good online habits benefits the global digital community.
- POST ONLINE ABOUT OTHERS AS YOU HAVE THEM POST ABOUT YOU: The Golden Rule applies online as well.
- HELP THE AUTHORITIES FIGHT CYBERCRIME: Report stolen finances or identities and other cybercrime to the Internet Crime Complaint Center (www.ic3.gov) and to your local law enforcement or state attorney general as appropriate.

OWN YOUR ONLINE PRESENCE

- PERSONAL INFORMATION IS LIKE MONEY. VALUE IT. PROTECT IT: Information about you, such as your purchase history or location, has value – just like money. Be thoughtful about who gets that information and how it's collected through apps and websites.
- BE AWARE OF WHAT'S BEING SHARED: Set the privacy and security settings on web services and devices to your comfort level for information sharing. It's OK to limit how and with whom you share information.
- SHARE WITH CARE: Think before posting about yourself and others online. Consider what a post reveals, who might see it and how it could be perceived now and in the future.

STOP | THINK | CONNECT™

RANSOMWARE FACTS & TIPS

As technology evolves, the prevalence of ransomware attacks is growing among businesses and consumers alike. It's important for digital citizens to be vigilant about basic digital hygiene in an increasingly connected world.

WHAT IS RANSOMWARE?

Ransomware is a type of malware that accesses a victim's files, locks and encrypts them and then demands the victim to pay a ransom to get them back. Cybercriminals use these attacks to try to get users to click on attachments or links that appear legitimate but actually contain malicious code. Ransomware is like the "digital kidnapping" of valuable data – from personal photos and memories to client information, financial records and intellectual property. Any individual or organization could be a potential ransomware target.

WHAT CAN YOU DO?

We can all help protect ourselves – and our organizations – against ransomware and other malicious attacks by following these STOP. THINK. CONNECT. tips:

- **Keep all machines clean:** Keep the software on all Internet-connected devices up to date. All critical software, including computer and mobile operating systems, security software and other frequently used programs and apps, should be running the most current versions.
- **Get two steps ahead:** Turn on two-step authentication – also known as two-step verification or multi-factor authentication – on accounts where available. Two-factor authentication can use anything from a text message to your phone to a token to a biometric like your fingerprint to provide enhanced account security.
- **Back it up:** Protect your valuable work, music, photos and other digital information by regularly making an electronic copy and storing it safely.
- **Make better passwords:** A strong password is a sentence that is at least 12 characters long. Focus on positive sentences or phrases that you like to think about and are easy to remember.
- **When in doubt, throw it out:** Links in email, social media posts and online advertising are often how cybercriminals try to steal your personal information. Even if you know the source, if something looks suspicious, delete it.
- **Plug & scan:** USBs and other external devices can be infected by viruses and malware. Use your security software to scan them.

Created by the National Cyber Security Alliance

STOPTHINKCONNECT.ORG

@STOPTHNKCONNECT STOPTHINKCONNECT STOPTHINKCONNECT

STOP | THINK | CONNECT™

SAFETY TIPS FOR MOBILE DEVICES

Stay #CyberAware While On the Go

Your mobile devices – including smartphones, laptops and tablets – are always within reach everywhere you go, whether for work, travel or entertainment. These devices make it easy to connect to the world around you, but they can also pack a lot of info about you and your friends and family, like your contacts, photos, videos, location and health and financial data. It's important to use your mobile device safely.

The first step is to STOP. THINK. CONNECT.

STOP: make sure security measures are in place. THINK: about the consequences of your actions and behaviors online. CONNECT: and enjoy your devices with more peace of mind.

PERSONAL INFORMATION IS LIKE MONEY. VALUE IT. PROTECT IT.

- **Secure your devices:** Use strong passwords or touch ID features to lock your devices. These security measures can help protect your information if your devices are lost or stolen and keep prying eyes out.
- **Think before you app:** Information about you, such as the games you like to play, your contacts list, where you shop and your location, has value – just like money. Be thoughtful about who gets that information and how it's collected through apps.
- **Now you see me, now you don't:** Some stores and other locations look for devices with WiFi or Bluetooth turned on to track your movements while you are within range. Disable WiFi and Bluetooth when not in use.
- **Get savvy about WiFi hotspots:** Public wireless networks and hotspots are not secure, which means that anyone could potentially see what you are doing on your mobile device while you are connected. Limit what you do on public WiFi and avoid logging in to key accounts like email and financial services on these networks. Consider using a virtual private network (VPN) or a personal/mobile hotspot if you need a more secure connection on the go.

KEEP A CLEAN MACHINE:

- **Keep your mobile devices and apps up to date:** Your mobile devices are just as vulnerable as your PC or laptop. Having the most up-to-date security software, web browser, operating system and apps is the best defense against viruses, malware and other online threats.
- **Delete when done:** Many of us download apps for specific purposes, such as planning a vacation, and no longer need them afterwards, or we may have previously downloaded apps that are no longer useful or interesting to us. It's a good security practice to delete all apps you no longer use.

Created by the National Cyber Security Alliance
Made possible in whole by a grant fron the Digital Trust Foundation

STOPTHINKCONNECT.ORG

@STOPTHNKCONNECT STOPTHINKCONNECT STOPTHINKCONNECT

PARA | PIENSA | CONÉCTATE®

CONSEJOS Y RECOMENDACIONES

Para. Piensa. Conectate.™ es la educación nacional de ciberseguridad y la campaña de sensibilización.

Consejo: mantenga limpia su computadora.

- **Mantenga actualizado el software de seguridad:** tener actualizados el software de seguridad, el navegador web y el sistema operativo son las mejores defensas contra virus, software malicioso y otras amenazas en línea.

- **Automatice las actualizaciones de software:** muchos programas de software se conectarán y actualizarán de forma automática para defenderse contra riesgos conocidos. Active las actualizaciones automáticas si esta es una opción disponible.

- **Proteja todos los dispositivos que se conectan a Internet:** además de las computadoras, los teléfonos inteligentes, los sistemas de juegos y otros dispositivos web también necesitan protección contra virus y software malicioso.

- **Conecte y analice:** los dispositivos USB y otros dispositivos externos se pueden infectar con virus y software malicioso. Use su software de seguridad para analizarlos.

Consejo: proteja su información personal.

- **Proteja sus cuentas:** pida protección adicional de las contraseñas. Muchos proveedores de cuentas ofrecen actualmente formas extras de verificar su identidad antes de realizar negocios en ese sitio.

- **Cree contraseñas largas y seguras:** combine letras en mayúscula y minúscula con números y símbolos para crear una contraseña más segura.

- **Cuenta única, contraseña única:** las contraseñas separadas para cada cuenta ayudan a frustrar los ataques informáticos.

- **Escríbala y protéjala:** todos podemos olvidar una contraseña. Mantenga una lista en un lugar seguro alejado de su computadora.

- **Controle su presencia en línea:** cuando sea posible, configure los parámetros de privacidad y seguridad en los sitios web al nivel de confianza deseado cuando comparta información. Es correcto limitar con quién comparte su información.

Created by the National Cyber Security Alliance

CONSEJOS Y RECOMENDACIONES

PARA | PIENSA | CONÉCTATE®

Consejo: conéctese con cuidado.

- **Ante la duda, es mejor eliminar:** los enlaces en los correos electrónicos, tweets, publicaciones y anuncios en línea son, a menudo, la forma que utilizan los atacantes cibernéticos para poner enriesgo su computadora. Si es sospechoso, aun si conoce de donde proviene, es mejor eliminarlo o, si corresponde, marcarlo como correo electrónico no deseado.

- **Conozca las zonas de cobertura Wi-Fi:** limite el tipo de transacciones que realiza y ajuste los parámetros de seguridad en su dispositivo para limitar quién tiene acceso a su computadora.

- **Proteja su dinero:** si realiza compras o transacciones bancarias, compruebe que el sitio tenga activada la seguridad. Busque direcciones web con “https://” o “shttp://”, lo que significa que el sitio toma medidas adicionales para mantener la seguridad de su información. “Http://” no es seguro.

Consejo: manténgase informado sobre la web.

- **Manténgase actualizado. Esté al tanto de las formas nuevas de mantenerse protegido en línea.** Visite los sitios web confiables para obtener la información más reciente y compartirla con amigos, familiares y colegas, y recomendarles que conozcan el funcionamiento de la web.

- **Piense antes de actuar:** desconfíe de las comunicaciones que le piden que actúe de inmediato, que ofrecen algo demasiado bueno para ser verdad o que piden información personal.

- **Haga copias de respaldo:** proteja su trabajo, música, fotos y demás información digital valiosa mediante una copia electrónica y guárdela en un lugar seguro.

Consejo: sea un buen ciudadano virtual.

- **Seguro para mí, seguro para todos:** lo que hace en línea puede afectar a todos en el hogar, en el trabajo o alrededor del mundo. La práctica de buenos hábitos en línea favorece a toda la comunidad digital.

- **Publique información sobre otros de la misma manera que ellos publican sobre usted.**

- **Ayude a las autoridades a luchar contra el delito informático:** informe sobre identidades o finanzas robadas u otros delitos informáticos a http://www.ic3.gov/ (Centro de reclamaciones sobre delitos en Internet, Internet Crime Complaint Center), la Comisión Federal de Comercio (Federal Trade Commission) en http://www.ftc.gov/complaint (si se trata de un fraude), y a la autoridad competente o fiscalía local, según corresponda.

Created by the National Cyber Security Alliance

TECHNOLOGY CHECKLIST

Businesses are quickly deploying all kinds of technology. Different kinds of technologies come with different risks and strategies to protect them. This checklist is designed to help you identify the technology in your business you need to protect. In addition, there are some basic security tips, considerations and links to resources that can help you learn more to detect, respond to and recover from cyber incidents.

- ☐ WIFI
- ☐ ROUTERS
- ☐ FIREWALLS
- ☐ MOBILE DEVICES
- ☐ EMAIL
- ☐ FILE SHARING
- ☐ COPIERS/PRINTERS/FAX MACHINES
- ☐ CLOUD SOLUTIONS
- ☐ VPN
- ☐ SWITCHES
- ☐ USB
- ☐ WEBSITE
- ☐ SOCIAL NETWORKING
- ☐ POINT OF SALE
- ☐ 3RD PARTY VENDORS

WIFI:

- Use strong administrative and network access passwords
- Use strong encryption (WPA2 and AES encryption)
- Use separate WiFi for guests
- Physically secure WiFi equipment
- Get savvy about WiFi hotspots – Limit accessing sensitive information on public WiFi – Use VPN when using public WiFi

VIRTUAL PRIVATE NETWORK (VPN):

- Use strong passwords, authentication and encryption
- Limit access to those with valid business need
- Provide strong antivirus protection to users

NETWORK DEVICES:

Routers and Switches

- Use a network monitoring app to scan for unwanted users
- Restrict remote administrative management
- Log out after configuring
- Keep firmware updated
- Use strong passwords

Firewalls

- Default rules should block everything that is not specifically necessary for the business

USBs:

- Scan USBs and other external devices for viruses and malware when connected
- Only pre-approved USBs allowed in company devices
- Educate users about USB risks

STOP | THINK | CONNECT™

WEBSITE:

- Keep software up to date
- Require users to create strong passwords to access
- Prevent direct access to upload files to site
- Use scan tools to test your site's security – many are free
- Register sites with similar spelling to yours
- Run most current versions of content management systems or require web administrator/hosts to do the same

MOBILE DEVICES:

- Keep a clean machine: Update security software on all devices
- Delete unneeded apps
- Secure devices with passcodes or other strong authentication such as a finger swipe and keep physically safe
- Encrypt sensitive data on all devices
- Make sure "find device" and "remote wipe" are activated

EMAIL:

- When in doubt, throw it out: Educate employees about remaing alert to suspicious email
- Provide all email recipients with an option to opt off your distribution list
- Require long, strong and unique passwords on work accounts
- Get two steps ahead: Turn on two-factor authentication

FILE SHARING:

- Restrict the locations to which work files containing sensitive information can be saved or copied
- If possible, use application-level encryption to protect the information in your files
- Use file-naming conventions that are less likely to disclose the types of information a file contains
- Monitor networks for sensitive information, either directly or by using a third-party service provider
- Free services do not provide the legal protection appropriate for business

SOCIAL NETWORKING:

- Create page manager policies and roles
- Limit administrative access
- Require two-factor authentication
- Secure mobile devices

CLOUD AND OTHER 3RD PARTY VENDORS:

- Discuss the approach to security and codify in any agreements and contracts

POINT OF SALE (POS):

- Make unique, strong and long passwords and change regularly
- Separate user and administrative accounts
- Keep a clean machine: Update hardware and software as needed
- Avoid web browsing on POS terminals
- Use antivirus protection

COPIERS/PRINTERS/FAX MACHINES:

- Understand that digital copiers/printers/fax machines are computers
- Ensure devices have encryption and overwriting
- Take advantage of all the security features offered
- Secure/wipe the hard drive before disposing of an old device
- Disable the web management interface or change the default password

OTHER:

Secure Disposal

- Be aware that many devices, not just PCs and phones, have memory. Know how to clean old data before disposing

Internet of Things (IoT)

Consumer Protection and Defense Recommendations

- Isolate IoT devices on their own protected networks and change default passwords
- Know what information is being collected and how and where it's being stored and protected
- Consider whether IoT devices are ideal for their intended purpose
- Purchase IoT devices from manufacturers with a track record of providing secure devices
- When available, update IoT devices with security patches

(Source: www.ic3.gov)

Consumer Reports –
Privacy Tips for the Internet of Things
http://www.ic3.gov/media/2015/150910.aspx

FTC – Careful Connections:
Building Security in the Internet of Things
http://1.usa.gov/1Vgftep

STOP | THINK | CONNECT™

DATA BREACH RESPONSE

A Guide for Business

Federal Trade Commission | business.ftc.gov

You just learned that your business experienced a data breach. Whether hackers took personal information from your corporate server, an insider stole customer information, or information was inadvertently exposed on your company's website, you are probably wondering what to do next.

What steps should you take and whom should you contact if personal information may have been exposed? Although the answers vary from case to case, the following guidance from the Federal Trade Commission (FTC) can help you make smart, sound decisions.

This guide addresses the steps to take once a breach has occured. For advice on implementing a plan to protect consumers' personal information, to prevent breaches and unauthorized access, check out the FTC's *Protecting Personal Information: A Guide for Business* and *Start with Security: A Guide for Business.*

Secure Your Operations

Move quickly to secure your systems and fix vulnerabilities that may have caused the breach. The only thing worse than a data breach is multiple data breaches. Take steps so it doesn't happen again.

Mobilize your breach response team right away to prevent additional data loss. The exact steps to take depend on the nature of the breach and the structure of your business.

Assemble a team of experts to conduct a comprehensive breach response. Depending on the size and nature of your company, they may include forensics, legal, information security, information technology, operations, human resources, communications, investor relations, and management.

- **Identify a data forensics team.** Consider hiring independent forensic investigators to help you determine the source and scope of the breach. They will capture forensic images of affected systems, collect and analyze evidence, and outline remediation steps.
- **Consult with legal counsel.** Talk to your legal counsel. Then, you may consider hiring outside legal counsel with privacy and data security expertise. They can advise you on federal and state laws that may be implicated by a breach.

Secure physical areas potentially related to the breach. Lock them and change access codes, if needed. Ask your forensics experts and law enforcement when it is reasonable to resume regular operations.

Stop additional data loss. Take all affected equipment offline immediately— but don't turn any machines off until the forensic experts arrive. Closely monitor all entry and exit points, especially those involved in the breach. If possible, put clean machines online in place of affected ones. In addition, update credentials and passwords of authorized users. If a hacker stole credentials, your system will remain vulnerable until you change those credentials, even if you've removed the hacker's tools.

Remove improperly posted information from the web.

- **Your website:** If the data breach involved personal information improperly posted on your website, immediately remove it. Be aware that internet search engines store, or "cache," information for a period of time. You can contact the search engines to ensure that they don't archive personal information posted in error.
- **Other websites:** Search for your company's exposed data to make sure that no other websites have saved a copy. If you find any, contact those sites and ask them to remove it.

Interview people who discovered the breach. Also, talk with anyone else who may know about it. If you have a customer service center, make sure the staff knows where to forward information that may aid your investigation of the breach. Document your investigation.

Do not destroy evidence. Don't destroy any forensic evidence in the course of your investigation and remediation.

Fix Vulnerabilities

Think about service providers. If service providers were involved, examine what personal information they can access and decide if you need to change their access privileges. Also, ensure your service providers are taking the necessary steps to make sure another breach does not occur. If your service providers say they have remedied vulnerabilities, verify that they really fixed things.

Check your network segmentation. When you set up your network, you likely segmented it so that a breach on one server or in one site could not lead to a breach on another server or site. Work with your forensics experts to analyze whether your segmentation plan was effective in containing the breach. If you need to make any changes, do so now.

Work with your forensics experts. Find out if measures such as encryption were enabled when the breach happened. Analyze backup or preserved data. Review logs to determine who had access to the data at the time of the breach. Also, analyze who currently has access, determine whether that access is needed, and restrict access if it is not. Verify the types of information compromised, the number of people affected, and whether you have contact information for those people. When you get the forensic reports, take the recommended remedial measures as soon as possible.

Have a communications plan. Create a comprehensive plan that reaches all affected audiences — employees, customers, investors, business partners, and other stakeholders. Don't make misleading statements about the breach. And don't withhold key details that might help consumers protect themselves and their information. Also, don't publicly share information that might put consumers at further risk.

Anticipate questions that people will ask. Then, put top tier questions and clear, plain-language answers on your website where they are easy to find. Good communication up front can limit customers' concerns and frustration, saving your company time and money later.

Notify Appropriate Parties

When your business experiences a data breach, notify law enforcement, other affected businesses, and affected individuals.

Determine your legal requirements.

Most states, the District of Columbia, Puerto Rico, and the Virgin Islands have enacted legislation requiring notification of security breaches involving personal information. In addition, depending on the types of information involved in the breach, there may be other laws or regulations that apply to your situation. Check state and federal laws or regulations for any specific requirements for your business.

Notify Law Enforcement

Call your local police department immediately. Report your situation and the potential risk for identity theft. The sooner law enforcement learns about the theft, the more effective they can be. If your local police aren't familiar with investigating information compromises, contact the local office of the FBI or the U.S. Secret Service. For incidents involving mail theft, contact the U.S. Postal Inspection Service.

Did the breach involve electronic health information?

Then check if you're covered by the Health Breach Notification Rule. If so, you must notify the FTC and in some cases, the media. *Complying with the FTC's Health Breach Notification Rule* explains who you must notify, and when.

Also, check if you're covered by the HIPAA Breach Notification Rule. If so, you must notify the Secretary of the U.S. Department of Health and Human Services (HHS) and in some cases, the media. HHS's Breach Notification Rule explains who you must notify, and when.

Health Breach Resources

HIPAA Breach Notification Rule:

hhs.gov/hipaa/for-professionals/breach-notification

HHS HIPAA Breach Notification Form:

hhs.gov/hipaa/for-professionals/breach-notification/breach-reporting

Complying with the FTC's Health Breach Notification Rule:

ftc.gov/healthbreachnotificationrule

Notify Affected Businesses

If account access information—say, credit card or bank account numbers—has been stolen from you, but you don't maintain the accounts, notify the institution that does so it can monitor the accounts for fraudulent activity.

If you collect or store personal information on behalf of other businesses, notify them of the data breach.

If names and Social Security numbers have been stolen, contact the major credit bureaus for additional information or advice. If the compromise may involve a large group of people, advise the credit bureaus if you are recommending that people request fraud alerts and credit freezes for their files.

Equifax: equifax.com or 1-800-685-1111

Experian: experian.com or 1-888-397-3742

TransUnion: transunion.com or 1-888-909-8872

Notify Individuals

If you quickly notify people that their personal information has been compromised, they can take steps to reduce the chance that their information will be misused. In deciding who to notify, and how, consider:

- state laws
- the nature of the compromise
- the type of information taken
- the likelihood of misuse
- the potential damage if the information is misused

For example, thieves who have stolen names and Social Security numbers can use that information not only to sign up for new accounts in the victim's name but also to commit tax identity theft. People who are notified early can take steps to limit the damage.

When notifying individuals, the FTC recommends you:

- **consult with your law enforcement contact** about the timing of the notification so it doesn't impede the investigation.
- **designate a point person within your organization for releasing information**. Give the contact person the latest information about the breach, your response, and how individuals should respond. Consider using letters (see sample on page 10), websites, and toll-free numbers to communicate with people whose information may have been compromised. If you don't have contact information for all of the affected individuals, you can build an extensive public relations campaign into your communications plan, including press releases or other news media notification.
- **consider offering at least a year of free credit monitoring or other support** such as identity theft protection or identity restoration services, particularly if financial information or Social Security numbers were exposed. When such information is exposed, thieves may use it to open new accounts.

Most states have breach notification laws that tell you what information you must, or must not, provide in your breach notice. In general, unless your state law says otherwise, you'll want to:

- **clearly describe what you know about the compromise**. Include:
  - how it happened
  - what information was taken
  - how the thieves have used the information (if you know)

- what actions you have taken to remedy the situation
- what actions you are taking to protect individuals, such as offering free credit monitoring services
- how to reach the relevant contacts in your organization

Consult with your law enforcement contact about what information to include so your notice doesn't hamper the investigation.

- **Tell people what steps they can take, given the type of information exposed, and provide relevant contact information.** For example, people whose Social Security numbers have been stolen should contact the credit bureaus to ask that fraud alerts or credit freezes be placed on their credit reports and contact the IRS Identity Protection Specialized Unit at 1-800-908-4490. See IdentityTheft.gov/databreach for information on appropriate follow-up steps after a compromise, depending on the type of personal information that was exposed. Consider adding this information as an attachment to your breach notification letter, as we've done in the model letter on page 10.
- **Include current information about how to recover from identity theft.** For a list of recovery steps, refer consumers to IdentityTheft.gov.
- **Consider providing information about the law enforcement agency working on the case, if the law enforcement agency agrees that would help.** Identity theft victims often can provide important information to law enforcement.

- **Encourage people who discover that their information has been misused to file a complaint with the FTC, using IdentityTheft.gov.** This information is entered into the Consumer Sentinel Network, a secure, online database available to civil and criminal law enforcement agencies.
- **Describe how you'll contact consumers in the future.** For example, if you'll only contact consumers by mail, then say so. If you won't ever call them about the breach, then let them know. This information may help victims avoid phishing scams tied to the breach, while also helping to protect your company's reputation. Some organizations tell consumers that updates will be posted on their website. This gives consumers a place they can go at any time to see the latest information.

Model Letter

The following letter is a model for notifying people whose names and Social Security numbers have been stolen. When Social Security numbers have been stolen, it's important to advise people to place a free fraud alert on their credit reports. A fraud alert may hinder identity thieves from getting credit with stolen information because it's a signal to creditors to contact the consumer before opening new accounts or changing existing accounts.

Also, advise consumers to consider placing a credit freeze on their file.

[Name of Company/Logo] Date: [Insert Date]

NOTICE OF DATA BREACH

Dear [Insert Name]:
We are contacting you about a data breach that has occurred at [insert Company Name].

What Happened?

[Describe how the data breach happened, the date of the breach, and how the stolen information has been misused (if you know)].

What Information Was Involved?

This incident involved your [describe the type of personal information that may have been exposed due to the breach].

What We Are Doing

[Describe how you are responding to the data breach, including: what actions you've taken to remedy the situation; what steps you are taking to protect individuals whose information has been breached; and what services you are offering (like credit monitoring or identity theft restoration services).]

What You Can Do

We recommend that you place a fraud alert on your credit file. A fraud alert tells creditors to contact you before they open any new accounts or change your existing accounts. Call any one of the three major credit bureaus. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts. The initial fraud alert stays on your credit report for one year. You can renew it after one year.

Equifax: equifax.com or 1-800-685-1111

Experian: experian.com or 1-888-397-3742

TransUnion: transunion.com or 1-888-909-8872

Request that all three credit reports be sent to you, free of charge, for your review. Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Thieves may hold stolen information to use at different times. Checking your credit reports periodically can help you spot problems and address them quickly.

If your personal information has been misused, visit the FTC's site at IdentityTheft.gov to get recovery steps and to file an identity theft complaint. Your complaint will be added to the FTC's Consumer Sentinel Network, where it will be accessible to law enforcers for their investigations.

You also may want to consider contacting the major credit bureaus at the telephone numbers above to place a free credit freeze on your credit file. A credit freeze means potential creditors cannot get your credit report. That makes it less likely that an identify thief can open new accounts in your name.

We have enclosed a copy of *Identity Theft: A Recovery Plan*, a comprehensive guide from the FTC to help you guard against and deal with identity theft. We've also attached information from IdentityTheft.gov about steps you can take to help protect yourself from identity theft, depending on the type of information exposed.

Other Important Information

[Insert other important information here.]

For More Information

Call [telephone number] or go to [Internet website]. [State how additional information or updates will be shared/or where they will be posted.]

[Insert Closing]

[Your Name]

Consider attaching the relevant section from IdentityTheft.gov, based on the type of information exposed in the breach. This is for a data breach involving Social Security numbers. There is similar information about other types of personal information.

Optional Attachment

FEDERAL TRADE COMMISSION

IdentityTheft.gov

What information was lost or exposed?

Social Security number

- ☐ If a company responsible for exposing your information offers you free credit monitoring, take advantage of it.
- ☐ Get your free credit reports from annualcreditreport.com. Check for any accounts or charges you don't recognize.
- ☐ Consider placing a credit freeze. A credit freeze makes it harder for someone to open a new account in your name.
  - If you place a freeze, be ready to take a few extra steps the next time you apply for a new credit card or cell phone —or any service that requires a credit check.
  - If you decide not to place a credit freeze, at least consider placing a fraud alert.
- ☐ Try to file your taxes early — before a scammer can. Tax identity theft happens when someone uses your Social Security number to get a tax refund or a job. Respond right away to letters from the IRS.
- ☐ Don't believe anyone who calls and says you'll be arrested unless you pay for taxes or debt — even if they have part or all of your Social Security number, or they say they're from the IRS.
- ☐ Continue to check your credit reports at annualcreditreport.com. You can order a free report from each of the three credit reporting companies once a year.

For More Guidance From the FTC

This publication provides general guidance for an organization that has experienced a data breach. If you'd like more individualized guidance, you may contact the FTC at 1-877-ID-THEFT (877-438-4338). Please provide information regarding what has occurred, including the type of information taken, the number of people potentially affected, your contact information, and contact information for the law enforcement agent with whom you are working. The FTC can prepare its Consumer Response Center for calls from the people affected, help law enforcement with information from its national victim complaint database, and provide you with additional guidance as necessary. Because the FTC has a law enforcement role with respect to information privacy, you may seek guidance anonymously.

For additional information and resources, please visit business.ftc.gov.

Federal Trade Commission
business.ftc.gov
May 2019

Collaboration:

The Ultimate Cybersecurity Tool for Government

Introduction

Today's cybersecurity best practices and response frameworks are drawn from networking and information sharing on an international scale. Similarly, close collaboration with colleagues and appropriate partners can help CISOs craft a sound strategy for defending against cyberattacks.

The threat of smaller attacks

Government agencies lost more than $860 million dealing with ransomware attacks between 2018 and 2023.[1] On average, it took government organizations 14 days to recover from an incident.

Recovering from a breach isn't just about operations. It's about preparing for the next threat and restoring trust with constituents. For state and local governments and educational institutions, the damage to credibility after a breach may linger long after the organization restores operations.

For every large incident like Colonial Pipeline[2] or the city of Dallas,[3] there are hundreds of smaller, less visible attacks. For example, Washington County, Pennsylvania, paid a $350,000 ransom to hackers who had taken control of the county's network and stolen a large amount of sensitive data in February 2024.[4]

"Cybercriminals are willing to hit a whole bunch of small organizations for tens of thousands of dollars, with the occasional bigger payoff," says Mark Sangster, vice president and chief strategy officer of Adlumin, a cloud-based managed detection and response (MDR) platform. "I think that's a key lesson many organizations haven't learned."

As Sangster notes, statistics on the scope and extent of cyberattacks are almost certainly undercounts because many cyber incidents are not made public.

Five keys to a successful cyber plan

In any threat situation, success depends on a collaborative plan that involves taking the right actions before, during and after a threat.

Many of the common available threat response frameworks — such as NIST Cybersecurity Framework (CSF) 2.0 and CIS Critical Security Controls® v8 — boil down to the following five steps.

First, fully appreciate your assets. Know what data your organization has, how it's used and the full measure of the services your entity provides.

Second, understand the associated implications and obligations of those assets. Your data and services should be key drivers of your plan.

Third, build the appropriate security framework and response mechanism for your organization.

This step does not have to be as difficult as one might expect. Many government and education organizations already have a crisis plan — whether related to pandemics, natural disasters or power failures — and have identified the people who should be part of the response as well as how to set up a command center to gather intelligence. For a cyber plan, these organizations can simply add the appropriate technical elements to an existing crisis plan.

> **Cybersecurity is not an IT problem to solve. It is a business risk to manage."**
>
> **Mark Sangster,** *Vice President and Chief Strategy Officer, Adlumin*

Tabletop exercises can be particularly helpful in building those technical elements.

Fourth, include the appropriate parties.

"IT security leaders understand ones and zeros," Sangster says. "Organizational administrators and leaders understand dollars and cents, the obligations and the risks to the organization itself. You do not want technical people interpreting the significance of the business or human elements, nor vice versa."

Fifth, coordinate applicable reporting after an incident. For example, critical-infrastructure organizations must report certain cyberattacks to the Cybersecurity and Infrastructure Security Agency (CISA) within 72 hours of discovery. Ransomware payments must be reported within 24 hours.

The human element

Human behavior can affect your organization's ability to respond to a cyber incident. According to Sangster, managing the following leadership personas is key to building a collaborative, cohesive plan.

The hero – Determined to singlehandedly fix the problem

The martyr – Generally an IT person who feels like they're the ones who made a mistake

The hoarders – People who want to collect all the data, do an end run around the team and go straight to the boss with everything gathered

The lawyer – The person who keeps bringing up all the risks that need to be considered

Part of the CISO's responsibility is understanding how group dysfunctions and biases might manifest themselves, then empowering the team to make the best possible decisions rather than engage in finger-pointing and defensiveness.

Incident response relies on making excruciating decisions quickly with not enough information to go on. It's mapping a path for turning volatility, uncertainty, chaos and ambiguity (also known as VUCA) into the exact opposite: vision, understanding, clarity and action.

The benefits of partnership

Smart cyber-physical systems that agencies have built to digitize operations require a higher level of security. Many organizations do a cost-benefit analysis and decide it makes sense to partner with an MDR provider to keep their data, assets and networks secure.

"Cybersecurity is not an IT problem to solve. It is a business risk to manage," says Sangster. Working with a partner lets your team focus on higher-level strategy as the provider identifies system vulnerabilities, stops threats, reduces risk and automates compliance.

The right MDR partner can help you assemble a response team, navigate interpersonal communications, build a strategic response plan and maintain sound decision-making during crises.

"I once had a friend who was a quarterback in the NFL," says Sangster. "He told me the point of practicing wasn't to practice until you got the play right — it was to practice until you couldn't get the play wrong. Cybersecurity preparedness is the same way, and that's where a strong partner makes a difference."

1. https://www.comparitech.com/blog/information-security/government-ransomware-attacks/
2. https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years
3. https://www.axios.com/local/dallas/2023/05/16/dallas-city-cyberattack-ransomware
4. https://therecord.media/pennsylvania-county-pays-cyberattack-ransom

This piece was written and produced by the Government Technology Content Studio, with information and input from Adlumin.

Produced by Government Technology
Government Technology is about solving problems in state and local government through the smart use of technology. Government Technology is a division of e.Republic, the nation's only media and research company focused exclusively on state and local government and education.

www.govtech.com

Often Overlooked, **Printers Require Protection Strategies**

How prevention, authentication and modernization expand endpoint security

We rely on printing and document sharing so often it's easy to overlook the security vulnerabilities inherent to them. However, both pose significant risks.

Printers are usually connected to the organization's network, exposing them to the same vulnerabilities as other network devices. When workers at home or in the field connect remotely to print, scan or copy, the risk of breaches and cyberattacks is even greater.

"Printers and copiers have powerful processors, store information and integrate to line-of-business systems," says John Spiak, senior manager of solutions consulting at Canon. "However, organizations typically don't protect them in the same way they would a laptop or desktop workstation. These devices have become low-hanging fruit for cybercriminals."

Printers are usually connected to the organization's network, exposing them to the same vulnerabilities as other network devices.

Proactively Protect Your Printers

Agencies often find including printers, scanners and copiers in their organization-wide cybersecurity practices is an intuitive way to quickly improve their security posture. They just need to expand what they're already finding successful.

The first step for many organizations is regular training for all staff, which must include training on printer and scanner protection. And it's not enough to have employees take a course once per year.

"The risks and what cybercriminals are doing change daily," says Bill Rials, senior fellow for the Center for Digital Government. "Trainings should be at least monthly and in small chunks."

When it comes to technology, agencies should harden devices by closing unused ports. Changing the default administrator password that comes with each device should be a top priority.

"People don't always pay attention to what ports are open," Spiak says. "That's a huge threat vector when you consider your most critical business information passes through these devices on a daily basis."

IT teams must update printers and other firmware regularly to patch vulnerabilities and address new exploits just as they would other devices. Additionally, printer devices need to be included in security assessments and testing going forward.

The following strategies are also necessary to improve security:

Make integration a priority. Integrate devices with your security information and event management tools to help identify patterns in user and device behavior, detect potential breaches and respond quickly and decisively to alerts.

Establish configuration baselines. Each device may have dozens of controls users can turn off or adjust. Configuration baselines serve two functions. First, a device integrity check is activated when the device starts up. If the check detects malicious behavior or changes, it automatically returns the device to its baseline configuration. The second function standardizes security controls across printer fleets, simplifies management and accelerates recovery if printer configurations are deleted or corrupted.

Encrypt data at rest and in transit. Once an encrypted file reaches a device, the device should encrypt data during processing and purge the data from the device once a print, scan or other job is complete.

"The risks and what cybercriminals are doing change daily. Trainings should be at least monthly and in small chunks."

— Bill Rials, Senior Fellow,
Center for Digital Government

Deploy Authentication and Access Controls

Authentication protects sensitive information by verifying the identity of users. When used with role-based access control and principles of least privilege, it ensures users can only access documents and print functions they need to do their job. In addition, it enables auditing by attributing activity to a specific user and providing granular reporting on how the device is utilized (e.g., what time a person logged in or released their job or whether they changed device settings).

To prevent unauthorized reproduction, alteration, sharing or viewing of printed and digital documents, agencies should choose solutions that incorporate key components of a Zero Trust security framework. This approach requires that users continuously verify their identity as they access additional documents, apps or programs rather than relying on just one username and password combination to gain complete access.

In poorly secured environments, print jobs may remain in printer trays for hours or days, where anyone can maliciously or inadvertently view or take documents they're not entitled to. Requiring users to authenticate themselves before accessing documents protects this critical information.

Advanced print management solutions offer flexible authentication methods such as username/password, proximity-based cards and USB keys. They also allow users to apply watermarks to sensitive documents and set time limits on the availability of shared documents.

Modernize the Print Infrastructure

The print architecture in many organizations is based on management tools and utilities that have not been updated in years. These systems were not designed for today's security threats and are more prone to vulnerabilities.

Moving to cloud-based systems equips organizations with modern, secure-by-design tools that are regularly patched and updated by the cloud provider.

"The provider handles updates to firmware and certificates without requiring the intervention of the IT or print admin," says Aaron Hale, senior manager of vertical marketing for Canon. "It takes some of the burden off the resident IT team to focus on more critical things."

Another important benefit of leading cloud services is adherence and certification. The Federal Risk and Authorization Management Program (FedRAMP) uses National Institute of Standards and Technology guidelines to provide standardized security requirements for cloud services.

By independently verifying and monitoring monthly that a particular cloud service adheres to the requirements, they help reduce internal security evaluation requirements and provide a level of assurance that allows organizations to adopt cloud services more confidently.

Deploying these strategies as they fit for an organization immediately improves their security posture by protecting more endpoints and securing critical information.

This piece was written and produced by the Center for Digital Government Content Studio, with information and input from Canon.

Produced by the Center for Digital Government

The Center for Digital Government, a division of e.Republic, is a national research and advisory institute on information technology policies and best practices in state and local government. Through its diverse and dynamic programs and services, the Center provides public and private sector leaders with decision support, knowledge and opportunities to help them effectively incorporate new technologies in the 21st century.

www.centerdigitalgov.com.

Sponsored by Canon Solutions America

For more information, call 800-815-4000.

SHUTTERSTOCK.COM