BOISE METRO **CHAMBER**

CYBERSECURITY

SMALL BUSINESS **GUIDEBOOK**

SPONSORED BY

Idaho National Laboratory

IN PARTNERSHIP WITH

BOISE STATE UNIVERSITY
DIVISION OF RESEARCH AND ECONOMIC DEVELOPMENT
Institute for Pervasive Cybersecurity

TABLE OF CONTENTS

BOISE METRO **CHAMBER**

The Boise Metro Chamber respects the importance of effective cybersecurity to our businesses. It is imperative that we understand how cyberattacks threaten our businesses and how to protect ourselves from them. Therefore, we have adapted this information from trusted sites. These resources offer knowledge to help reduce the risks and safely enjoy the benefits of a global and open internet.

Because our member businesses differ and exist in different sectors, some of the information provided within this guidebook may or may not apply. Employers are encouraged to evaluate their cybersecurity procedures and seek additional expert guidance.[1; 2]

LETTER FROM THE CEO

Dear Chamber Members,

The ongoing COVID-19 pandemic impacts nearly every business in the Treasure Valley, and the economic impacts will have lasting effects. At the same time, law enforcement reports a massive increase in cybercrimes. Small businesses have a lot to worry about, and ensuring your data is secure should be at the top of your list.

Because cybersecurity is an elusive goal with many trade-offs, it can also be an intimidating topic. Fear or lack of awareness can prevent businesses from evaluating risks and taking suitable actions. This cybersecurity guidebook provides a simple set of steps designed to support our members. While members are our focus, every business owner and staff should consider using this document as a starting place for cybersecurity considerations.

The economic benefits that flow from greater access to knowledge, information, goods, and services are made possible by the worldwide internet. It needs to be trusted and secured. Therefore, the Boise Metro Chamber is pleased to provide businesses of all sizes with this simple, clear guide to addressing the increasingly serious challenge of cybersecurity.

Sincerely,

Bill Connors, President & CEO
Boise Metro Chamber
Boise Convention & Visitors Bureau
Boise Valley Economic Partnership

WHY CYBER SECURITY IS GOOD FOR IDAHO BUSINESSES

Increasingly, Idaho's economy is intertwined with the global economy, and our prosperity is dependent upon the security of our digital infrastructure. More and more Idahoans are conducting a majority of their business online, and the internet is critical to Idaho's $72.5 billion GDP. In 2010 (yes, 10 years ago) the Federal Communications Commission estimated that 97% of small businesses use email and 74% have a company website.

Because small businesses make up the backbone of Idaho's economy, they need hygienic cyber practices and simple tools to train and remind their employees of the cybersecurity issues they face. Most people want to protect themselves from cyberthreats, they just need the training and awareness to protect themselves, and thereby their employer. Cybersecurity is the practice of ensuring the integrity, confidentiality, and accessibility of information. Cybersecurity consists of an evolving set of tools, risk management approaches, technologies, processes, and best practices designed to protect networks, devices, programs, and data from attacks or unauthorized access.

In this day in age, most businesses or organizations have unprecedented amounts of data on computers and other devices. Some of the data can contain sensitive information for which unauthorized exposure could have negative consequences. As the volume of cyberattacks grow, businesses need to take steps to protect their sensitive business and personnel information.

We have shared some of the most common cyberattacks and how to prevent your business and yourself from being a target. We have also listed best practices when it comes to your employees and their understanding of cyberhygiene.

1. COMMON CYBERTHREATS

COMMON CYBERTHREATS

FRONT LINE & INITIAL ATTACKS

Social engineering is the art of exploiting human psychology — rather than technical hacking techniques — to gain access to buildings, systems, or data. These cyberattacks rely heavily on human interaction and involve manipulating victims into performing certain actions that break standard security practices.

There are technological solutions that help mitigate social engineering, such as email filters, firewalls, and network/data monitoring tools; however, extra steps towards educating employees on common types of social engineering attacks is the best defense against these schemes.

Examples Include:

Phishing — a type of online scam involving an email which claims to be from a legitimate business or known individual, but actually directs the recipient to a website which collects personal information for identity fraud. These emails often entice users to click on a link or open an attachment containing malicious code. After the code is run, your computer may become infected with malware.

SMishing — a variant of phishing that leverages SMS text messaging instead of email. With the prevalence of mobile phone usage and messaging platforms, the scammer has changed as well to find new victims. A simple text message is sent with a link. When the user clicks on the link, the phone's browser is redirected to a malicious site where malware is then sent to your phone. It has become a growing threat in the world of online security.

Spear phishing — By personalizing their phishing tactics, the scammer targets a specific individual or organization and by using personal information, gains the victim's trust and appears more legitimate. Spear phishers have a higher success rate of fooling their victims into divulging login credentials or sensitive information.

Baiting — Attackers perform baiting attacks when they leave a malware-infected device, such as a USB flash drive, in a place where someone will most likely find it. The success of the attack depends on that person connecting the device to their computer and in doing so, unknowingly installs the malware. Once installed, the attacker is able to advance into the victim's system.

Pretexting — Pretexting occurs when an attacker fakes circumstances to compel a victim into providing access to sensitive data or protected systems. Examples of pretexting attacks include a scammer pretending to need financial data in order to confirm the identity of the recipient. The scammer might also disguise themselves as a trusted entity, such as a member of the company's IT department in order to manipulate the victim into releasing and granting computer access.

Tailgating — Tailgating is a physical social engineering method that occurs when unauthorized individuals follow authorized individuals into a typically secured area. Tailgaters often take advantage of a helpful employee holding a door open for a visitor or someone without a badge. These lapses in security can negatively impact the organization by creating a potential data breach, financial loss through theft, or property damage, as well as destructing the organization's reputation.

Scareware — Scareware is a malware tactic that manipulates users into believing they need to download or buy malicious, sometimes useless, software. Most often initiated using a pop-up ad,

scareware uses social engineering to take advantage of a user's fear, coaxing them into installing fake antivirus software.

Social engineering is a serious and ongoing threat to many organizations and individuals. Education is the first step to prevent falling victim to clever attackers using increasingly sophisticated strategies to gain access to sensitive data.

VIRUSES, WORMS, AND TROJAN HORSES

Viruses, trojan horses, and worms are just a few terms used to describe malware. They are programs installed remotely to disable systems, acquire information, or gain access to internal systems.

Malware is software written with the intent to damage, exploit, or disable devices, systems, and networks. It is used to compromise device functions, steal data, bypass access controls, and cause harm to computers and other devices and the networks they are connected to.(It is often placed on a computer through social engineering tactics).

Ransomware is a type of malicious software that prevents you from accessing your computer files, systems, or networks and demands you pay a ransom for their return. Ransomware attacks can cause costly disruptions to operations and the loss of critical information and data.

Employees can unknowingly download malware or ransomware onto a computer by opening an email attachment, clicking an ad, following a link, or even visiting a website that's embedded with malware (often placed on a computer through a social engineering tool like phishing).

Once the code is loaded on a computer, it will lock access to the computer itself or data and files stored there. More menacing versions encrypt files and folders on local drives, attached drives, and even networked computers.

Most of the time, you don't know your computer has been infected. You usually discover it when you can no longer access your data or you see computer messages letting you know about the attack and demanding ransom payments.

A further complication of ransomware is that traditional antivirus software does not detect/eliminate it. Instead, there is a need to consider upgrading your end-point technology to include strong ransomware detection and response components.

BUSINESS EMAIL COMPROMISE (BEC)

Business email compromise (BEC) is one of the most financially damaging online crimes. It exploits the fact that so many of us rely on email to conduct business — both personal and professional.

BEC is a scam that relies heavily on social engineering tactics. Criminals send an email message that appears to come from a known source making a legitimate request. Attackers often impersonate CEOs or other high-ranking executives when implementing a BEC.

According to the FBI, these are three examples of BEC Attacks:

- A vendor your business regularly deals with sends an invoice with an updated mailing address.
- A company CEO asks an internal employee to purchase gift cards to send out as employee rewards. She asks for the serial numbers so she can email them out right away.
- A homebuyer receives a message from his title company with instructions on how to wire his down payment.

BUSINESS PROCESS COMPROMISE (BPC)

Business Process Compromise (BPC) is when an attacker alters some parts of specific business processes and attempts to compromise them for some financial gain. An attacker may try to silently watch internal communications and map out the normal process for a funds transfer. BPC can be a result of BEC (Business Email Compromise). Once they're in your system, they will add, modify, or delete key entries and/or intercept and modify transactions.

Payment security vulnerabilities are incredibly relevant today as cybercriminals continue to look for ways to exploit credit card information stored within business databases. The news tends to pick up stories about large companies who have been compromised, but small businesses are particularly vulnerable to these types of BPCs and they should be vigilant in taking precautions.

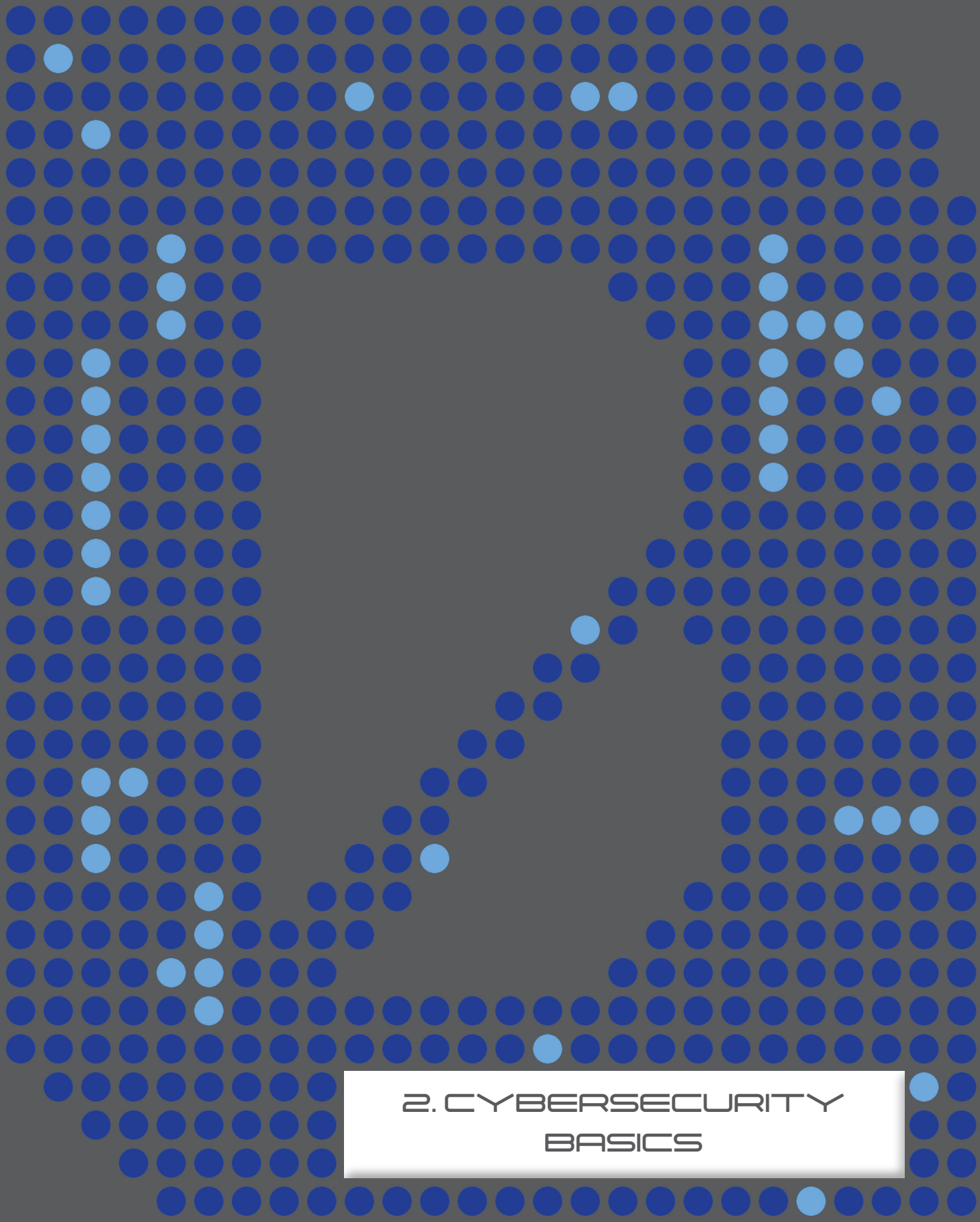
TELEWORK SECURITY ISSUES

COVID-19 created a new challenge for businesses in Idaho. Prior to 2020, less than one third of employees worked from home. That number has skyrocketed. And, accordingly, security issues from telework have increased similarly.

Remote employees are exposed to typical cyberthreats including phishing scams, malware, and ransomware attacks. Additionally, the decentralized approach to work has exposed the entire organization to additional threats from multiple entry points.

It is important for small businesses to consider this new challenge and re-up plans to remind and train employees to protect themselves. New telework internet security policies should be implemented for employees and additional considerations could include requiring access through a mobile hotspot rather than through public networks (like the local coffee shop).

Further, traditional on-site or remote colocation technologies we have relied upon — firewalls and antivirus for example — are being shown to be outdated in a telework environment. Growing small- and medium-sized businesses looking for silver linings of COVID-19 are looking to transform their IT platforms by moving from traditional infrastructure to online cloud and service providers. Those doing so should approach such efforts with an eye towards embedding security "at the start." End-point detection and response (EDR), multi-factor authentication (MFA), zero-trust networking (ATN), and cloud access security broker (CASB) technologies are just a few that support a transformation-focused IT model. However, just like legacy technologies, if improperly implemented or maintained, scammers and attackers will be breaking down your doors and trashing the investments you have made.



2. CYBERSECURITY BASICS

Cyberhygiene is comparable to personal hygiene. To maintain system health and improve online security, practices need to be put into place to ensure the safety of identity and sensitive information.

When it comes to cybersecurity and cyberhygiene, it's important to remember the three P's: *people, passwords, and patches*. People have a responsibility to know the risks of viruses and hacking and to also identify risks that could lead to being hacked. Passwords are the first line of defense against viruses and hackers. A patch is a small piece of software that a person or company issues whenever there is a security flaw.

PEOPLE

People are the linchpin to maintaining cyberhygiene. As an employer, your first line of defense against cyberattacks is your employee, **and they must be trained**. Most data breaches and exposure stem from human error. By accidentally downloading a malicious file, malware can be released into your internal network, thereby leaking sensitive and confidential documents. Awareness and a deeper understanding of cybersecurity protects you even more than a firewall or threat mitigation tool could.

Here are some cybersecurity tools to help create a safe environment for your employees as well as for your cybersystems:

- Ongoing professional cybersecurity education for employees is essential. Explain the impact a cyberattack may have on your organization's systems and networks. Make sure employees know the expectations of them to protect their passwords and devices.
- High-ranking executives and IT staff are targeted because of their access to extensive organizational information. Senior officials need to be aware of their vulnerabilities and take precautions.
- Encourage cooperation, not just compliance. Emplace a policy that covers potential attack vectors.
- Beware of social media, blogs, and suspicious links from unknown sources while at work or using corporate devices.
- Your employees should be trained before there is a cybersecurity attack issue and communicate a step-by-step plan on what to do if an incident occurs.

PASSWORDS

Passwords are required to login into almost everything you do online. Choosing a password that is both easy to remember and secure can be difficult, but below are some tips for keeping your password secure:

- Never give your password out to others.
- Use different passwords for different accounts.
- Use multi-factor authentication. This type of security includes an initial password and then another password or a set of numbers.
- Length is better than complex. Use at least 16 characters.
- Make passwords hard to guess but easy for you to remember. For example "cybersecurityguide" is both easy to remember and exceeds the 16 character recommendation.
- Use upper and lower case letters to increase complexity. Using special symbols such as % or # will further increase complexity.
- Consider using a password manager. (See list of recommendations for possible vendors.)
- If possible, activate multi-factor authentication (MFA) with your service providers (e.g. financial, health, supply chain).[3,4]

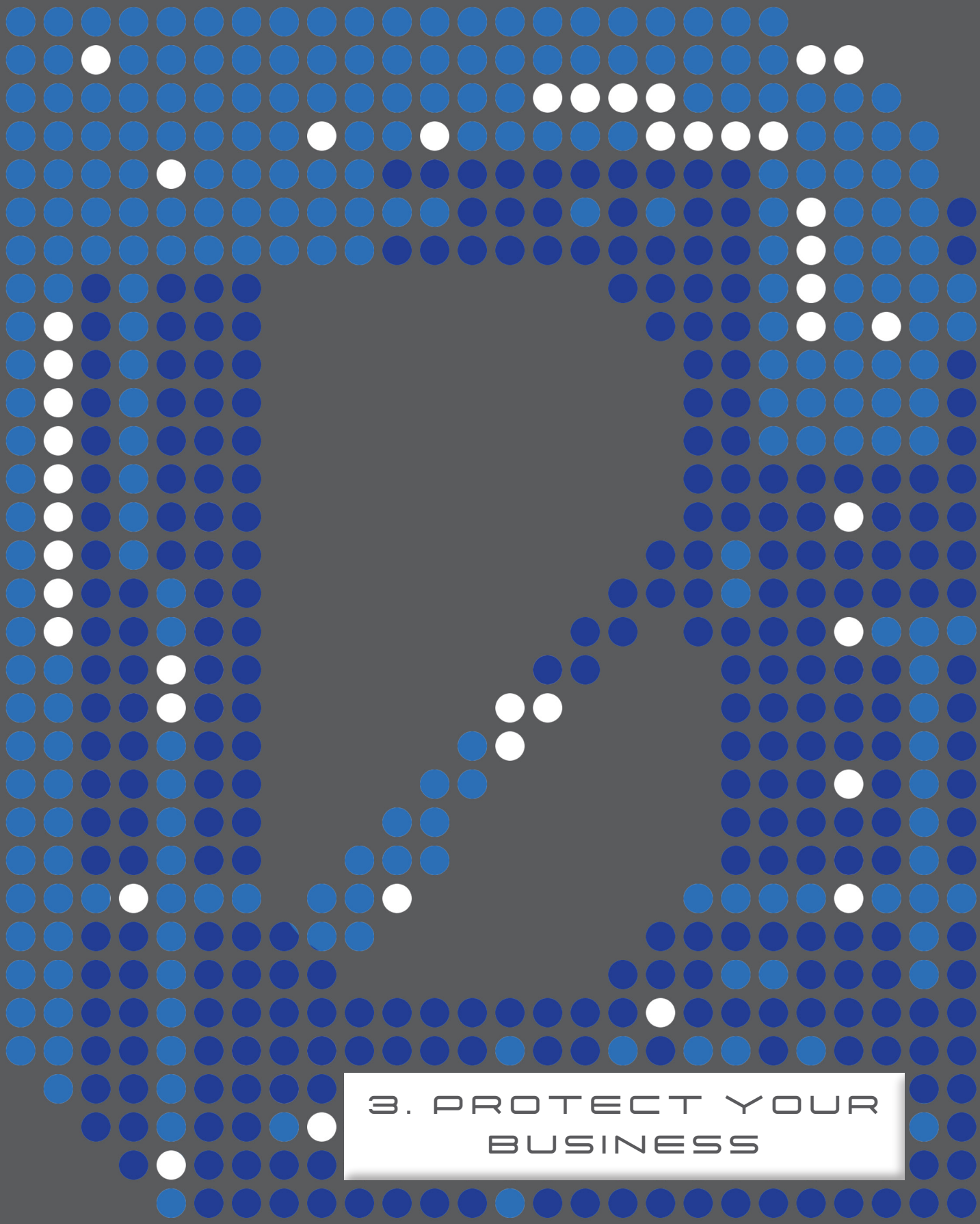
PATCHES

Patches cover the holes keeping hackers from further exploiting the flaw. Patches might also be built into your next device update. That's why it's very important to keep all of your software and handheld devices up-to-date. Keep your antivirus software updated and/or download recommended patches as soon as you are alerted.

Software updates whether big or small are important. Computers and the software they house require regular updates to ensure they continue to run safely and efficiently[5].

Below are five reasons why general software updates are important:

- Updates include repaired security holes and/or remove computer bugs.
- Software updates remove software vulnerabilities. Software vulnerabilities include security holes. Hackers can write code that targets these vulnerabilities.
- Software updates help to protect your data by ensuring your device is using the most up-to-date virus software.
- Updating your device not only protects you, but also protects those people and devices you communicate and share files with.
- Updates not only protect your device from viruses and/or hackers, but also ensure your device is running at top speed[6].



3. PROTECT YOUR BUSINESS

BUSINESS SECURITY CONSIDERATIONS

The consequences of any cyberattack can range from simple inconvenience to financial disaster. This guidebook was created to help improve cybersecurity within organizations and help raise awareness to better cyberhygiene. Though we know every situation is different and every business varies, here are some best practices and tips to ensure secure systems and protected business data.

Here are a few ways you can prevent social engineering attacks:

- Educate your staff on cyberattacks and the importance of cybersecurity knowledge and awareness.
- Always be aware of someone behind you, especially when entering a secure or restricted area.
- Report any suspicious behavior or persons.
- Do not reply to emails or click on pop-up messages that ask for personal or financial information. Legitimate businesses do not ask for this type of information online.
- Do not use email for personal or financial data. Email is not secure enough to transmit personal information. Use only a secured web transaction or postal mail when sending sensitive data to a known company.
- Be suspicious of unsolicited phone calls, visits, or email messages. If you receive an unsolicited request, try to verify the identity of the solicitor directly with the company.
- Ensure that you are going to the correct website. Type the website link (URL) directly into your web browser. Malicious web sites might look identical to legitimate sites.
- Upon being given or finding a device, be wary of inserting it into your computer before questioning where it came from.

Three Steps to Resilience Against Malware and Ransomware

1. Back Up Your Systems – Now (and Daily)

Immediately and regularly back up all critical and system configuration information on a separate device and store the backups offline, verifying their integrity and restoration process. If recovering after an attack, restore a stronger system than you lost, fully patched and updated to the latest version.

2. Reinforce Basic Cybersecurity Awareness and Education

Ransomware attacks often require the human element to succeed. Refresh employee training on recognizing cyberthreats, phishing, and suspicious links — the most common vectors for ransomware attacks. Remind employees of how to report incidents to appropriate IT staff in a timely manner, which should include out-of-band communication paths.

3. Revisit and Refine Cyber Incident Response Plans

Your organization must have a clear plan to address attacks when they occur, including when internal capabilities are overwhelmed. Make sure response plans include how to request assistance from external cyber first responders, such as local law enforcement, FBI, or other digital forensic and incident response (DFIR) companies with strong experience helping businesses of your size and maturity.

After implementing these recommendations, refer to the ransomware best practices published by the SBA[7], or the National Institute of Standards and Technology (NIST)[8] for additional steps to protect your organization.

How to Protect Your Business From Business Email Compromise

- Be careful with what information you share online via social media or other outlets. When you share things like pet names, schools you attended, links to family and friends, and your birthday, you can give a scammer all the information they need to guess your password or answer your security questions.
- Don't click on anything in an unsolicited email or text message asking you to update or verify account information. Look up the company's phone number on your own and call the company to ask if the request is legitimate and authorized.
- Carefully examine the email address, URL, and spelling used in any correspondence. Slight variations on familiar and legitimate addresses are used to fool you and gain your trust.
- Be careful what you download. Never open an email attachment from someone you don't know, and be wary of email attachments forwarded to you.
- Set up multi-factor authentication (MFA) on any account that allows it, and never disable it.
- Do not use the same password for multiple sites. This can be a tedious effort, so consider downloading or using a password manager. Wikipedia describes password managers as "a computer program that allows users to store, generate, and manage their personal passwords for online services. A password manager assists in generating and retrieving complex passwords, potentially storing such passwords in an encrypted database or calculating them on demand."
- Verify payment and purchase requests in person if possible or by calling the person to make sure it is legitimate. You should verify any change in account number or payment procedures with the person making the request.
- Be especially wary if the requestor is pressing you to act quickly.

How to Keep Your Business and Processes Secure

Organizations should understand and know when the system is operating normally and detect any abnormal operations. With that knowledge, the organization is capable of identifying any malicious activity within the system early enough.

Perform risk assessments with a third-party vendor. Most attacks target the transactional process between vendors and suppliers since this is where they usually expect a weak link to perpetuate the system.

Treat the inside of your network like it is as insecure as the internet. Recognize that your networks are still hackable and try to prevent any unauthorized movement from various systems, like payroll, account management, and manufacturing operations.

Educate and train employees to detect usual and unusual behaviors within the system and in the processes. Employees should have a clear understanding and be able to identify social engineering attacks.

The organization should have a strong network security policy that defines the interaction of every organizational member with the network system.

FCC PLANNING TOOL

The Federal Communications Commission offers a cybersecurity planning tool[9] to help you build a strategy based on your unique business needs.

CYBER RESILIENCE REVIEW

The Department of Homeland Security's (DHS) Cyber Resilience Review[10] (CRR) is a non-technical assessment to evaluate operational resilience and cybersecurity practices. You can either do the assessment yourself, or request a facilitated assessment[11] by DHS cybersecurity professionals.

CYBERHYGIENE VULNERABILITY SCANNING

DHS also offers free cyberhygiene vulnerability scanning[12] for small businesses. This service can help secure your internet-facing systems from weak configuration and known vulnerabilities. You will receive a weekly report for your action[13].

PHISHING RESOURCES

How Not to Get Hooked by a Phishing Scam[14]

Wide-ranging tips to help you avoid getting hooked by a phishing scam and subsequently losing your personal information. Provided by the Federal Trade Commission.

Avoid a Phishing Attack[15]

Extensive guidelines how to avoid social engineering and phishing attacks; explains the common methods that attackers use to steal your personal information. Provided by the U.S. Computer Emergency Response Team.

Anti-Phishing Working Group[16]

Information on how to eliminate fraud and identity theft that result from phishing, "pharming," and email spoofing of all types.[17; 18]

STATISTICS

Here are some of the study's key findings based on SMBs' responses[19]

38% — Allocating $1,000 or less to their IT security budget, compared to 29% in 2019 and 27% in 2018

78% — SMB employees temporarily working remotely

56% — May keep some positions permanently remote

32% — Identify budget as their greatest barrier, followed by employees who do not follow IT security guidelines (24%) and limited time to research and understand emerging threats (13%)

82% — Antivirus protection is the most important feature in a cybersecurity solution, followed by (57%), endpoint security (48%), archiving management and backup and VPN technologies, (47%), and web filtering (40%)

71% — Firewall on website rather than in the cloud

45% — Adjusted or reevaluated their IT security road map based on recent security breaches and ransomware attacks

15% — Stopped a data breach or any unauthorized access in the last 12 months before sensitive data was extracted

50% of American workers work for small businesses

Almost **60%** of breaches occur through organized crime

61% of businesses suffering a data breach had less than 1,000 employees

50% of businesses have over 1,000 pieces of unprotected sensitive data

Email is responsible for **92%** of malware infections

75% of all legitimate websites have unpatched vulnerabilities

40% of all cyberattacks are against small businesses

85% of subjects and actors were in the same country

70% of attacks are from external actors and 30% from internal

RELATED FBI NEWS AND MULTIMEDIA

Public Service Announcements from IC3

04.06.2020 | Cyber Criminals Conduct Business Email Compromise Through Exploitation of Cloud-Based Email Services, Costing U.S. Businesses More Than $2 Billion
Cyber criminals are targeting organizations that use popular cloud-based email services to conduct BEC scams.

09.10.2019 | Business Email Compromise: The $26 Billion Scam
Business email compromise/email account compromise is a sophisticated scam that targets both businesses and individuals who perform legitimate transfer-of-funds requests.

10.24.2018 | Business Email Compromise: Gift Cards
The Internet Crime Complaint Center (IC3) received an increase in the number of BEC complaints requesting victims purchase gift cards.

06.11.2018 | Business Email Compromise Contributes to Large-Scale Business Losses Nationwide
BEC schemes have cost victims billions of dollars in fraud losses over the last five years. This activity is a pervasive threat with significant financial losses and a considerable global impact.

04.13.2020 | FBI Warns of Advance Fee and BEC Schemes Related to Procurement of PPE and Other Supplies During COVID-19 Pandemic
The FBI is warning government and health care industry buyers of rapidly emerging fraud trends related to procurement of personal protective equipment (PPE), medical equipment such as ventilators, and other supplies or equipment in short supply during the current COVID-19 pandemic.

04.06.2020 | FBI Anticipates Rise in Business Email Compromise Schemes Related to the COVID-19 Pandemic
There has been an increase in BEC frauds targeting municipalities purchasing personal protective equipment or other supplies needed in the fight against COVID-19.

07.16.2020 | Money Mule Reined In
When a Texas school district fell victim to a $2 million business email compromise scheme, a Florida man moved much of the stolen money away from law enforcement's grasp — and is now spending time behind bars.

01.28.2020 | Sentence in BEC Scheme
A leader of a business email compromise ring that stole more than $120 million from two American companies is spending time behind bars. Learn how to protect yourself from this growing crime.

09.10.2019 | Operation reWired
The FBI worked with partner agencies domestically and in multiple countries around the world in a large-scale, coordinated effort to dismantle international business email compromise (BEC) schemes.

06.11.2018 | International BEC Takedown
The FBI partnered with domestic and international law enforcement agencies on Operation WireWire, a large-scale, coordinated effort to dismantle business email compromise schemes.

03.08.2018 | FBI, This Week: W-2 Phishing Scams Increase During Tax Season
The latest evolution of the sophisticated business email compromise scam targets businesses for access to sensitive tax-related data.

12.07.2017 | FBI, This Week: Criminals Put Holiday Spin on Internet-Facilitated Schemes
The FBI says criminals put a holiday twist on the methods they use to scam you online during this time of year.

11.09.2017 | FBI Chicago Warns Area Business Owners of Business Email Compromise Scam
FBI Chicago has important information for area business owners who find themselves the victim of a business email compromise (BEC) scam.

02.27.2017 | Business Email Compromise
The organized crime groups that perpetrate the financial cyber fraud called business email compromise have victimized companies and organizations around the world.

10.26.2016 | PSA: Business Email Compromise Scam
Public service announcement warning of the dangers of business email compromise scams (BECs).

10.07.2016 | Business Email Compromise Scams Cost Businesses Billions of Dollars
BEC scams involves the compromise of legitimate business and email accounts for the purpose of conducting unauthorized wire transfers.

07.27.2016 | OPS Business Email Compromise Guide
A guide providing best practices on what to do to safeguard the email system of a business from being compromised.

08.28.2015 | Business Email Compromise
A sophisticated scam is costing companies worldwide millions of dollars.

ENDNOTES

1. https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/business-email-compromise
2. https://cybersecurity.idaho.gov/
3. https://www.it.ucsb.edu/secure-compute-research-environment-user-guide/password-best-practices
4. https://www.plesk.com/blog/various/password-security-standards-in-2020/
5. https://cybersecurity.yale.edu/patchyourdevices
6. https://us.norton.com/internetsecurity-how-to-the-importance-of-general-software-updates-and-patches.html
7. https://www.sba.gov/business-guide/manage-your-business/stay-safe-cybersecurity-threats
8. https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7621r1.pdf
9. https://www.fcc.gov/cyberplanner
10. https://us-cert.cisa.gov/resources/assessments
11. https://us-cert.cisa.gov/resources/assessments#two-options
12. https://us-cert.cisa.gov/resources/ncats
13. https://www.sba.gov/business-guide/manage-your-business/stay-safe-cybersecurity-threats
14. https://www.consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams
15. https://us-cert.cisa.gov/ncas/tips/ST04-014
16. https://apwg.org/
17. https://cybersecurity.idaho.gov/cyber-hygiene/phishing-scams/
18. https://cybersecurity.idaho.gov/training/
19. https://www5.untangle.com/2020smbitsecurityreport

Special thanks to Tori Thomas, Alex Finney, and Connor Jay Liess from the Boise Metro Chamber for doing the research, compiling relevant info, and laying out a user-friendly document for our members. Additionally, thank you to Edward Vasko and Sin Ming Loo from Boise State University for their support in the development of this guide.

NOTES:

BOISE METRO **CHAMBER**

CYBERSECURITY

SMALL BUSINESS **GUIDEBOOK**

SPONSORED BY

Idaho National Laboratory

IN PARTNERSHIP WITH

BOISE STATE UNIVERSITY
DIVISION OF RESEARCH AND ECONOMIC DEVELOPMENT
Institute for Pervasive Cybersecurity