If You Connect IT, Protect IT!

Cybersecurity Tips to Protect Your Business

infoaxis

#BECYBERSMART

In This eBook

INTRODUCTION

Technology has evolved. So have cyber threats.

Technology has rapidly evolved and so have the extent of risks we face operating online. At Infoaxis, we understand that protecting your critical data is essential, which is why we have developed this eBook.

Here you will find tips and tools you can use to be proactive in keeping your personal and company devices and data secure from hackers and cybersecurity breaches.

If You Connect IT, Protect IT

Be it for our personal use or for business purposes, most of us are connecting to networks and interacting with some form of sensitive data on a daily basis. We have all kinds of great devices (such as phones, tablets, and PCs) that we're using to connect to a variety of networks, for instance, home, public Wi-Fi in the coffee shop, in our doctor's office, and at our place of work. Each has a different level of protection – or may have none at all.

Any one of these networks could be the target of a hacker, putting us and our sensitive information at risk. Think of the many things we're doing while connecting in these places, the applications we're using (examples at left), and the information we're accessing.

Regardless of where or why we're connecting, we need to take adequate measures to ensure we're protecting ourselves and our information.

Your Devices Need Security Software

No matter what type of device you're using, if you connect it, protect it. PCs, smartphones, tablets, and even gaming devices, are all network connected, sending and receiving information to and from the Internet.

Your device is likely loaded up with many different software applications. ***But does it have software installed to keep it protected from viruses and malware or for encrypting and protecting your connection to the Internet?*** Anti-virus, VPN, and firewall software all have something to offer as part of a layered security approach.

There are many security software options out there, including many free ones, that can quickly add a layer of security and protection to your devices. Many options are quick to install and easy to set up, even for the less tech-savvy among us. For business users, there are many options that are easy to manage, on-premises, or in the cloud—we can help you find one that works in your environment.

BONUS TIP

Even when using security software, you should also make sure your other apps are up to date with the latest versions (especially those that regularly connect to the Internet) and that they provide some level of security or encryption if they're used to access sensitive data. Many of these apps will notify you when an update becomes available. Many breaches occur when unpatched applications are exploited.

Is Your Web Browser Vulnerable?

Be sure to keep your preferred Web browser patched and up-to-date as well. Many attackers target known vulnerabilities in older browsers that can be fixed with a patch. Leaving these vulnerabilities in place just increases your attack surface and, unfortunately, makes you a more likely target.

Also practice safe Web surfing, like checking for **“https”** versus **“http”** when visiting websites (the **“s”** is for **“secure”**). This is often indicated in your browser with a padlock (sometimes green in color) next to the Web address. This means that your browser is using a secure connection and your communications are being encrypted. And remember, if it’s not encrypted, others may be able see your data, especially when using free public Wi-Fi.

Your Operating Systems Are at Risk Too

It's also important to make sure you're keeping your device's operating system (OS) patched and up-to-date. These patches often contain security fixes that help protect you from new threats, and many devices have an option to download new patches automatically as they're released.

Another thing to consider: **if your device is no longer capable of running the latest patches or OS versions, you could be putting your information at risk.** Most software developers continue to support and patch older versions of their OS for a length of time even after releasing newer versions. Knowing when that support ends is important, as you'll no longer receive those patches and security fixes, and you should consider whether or not to continue using the device.

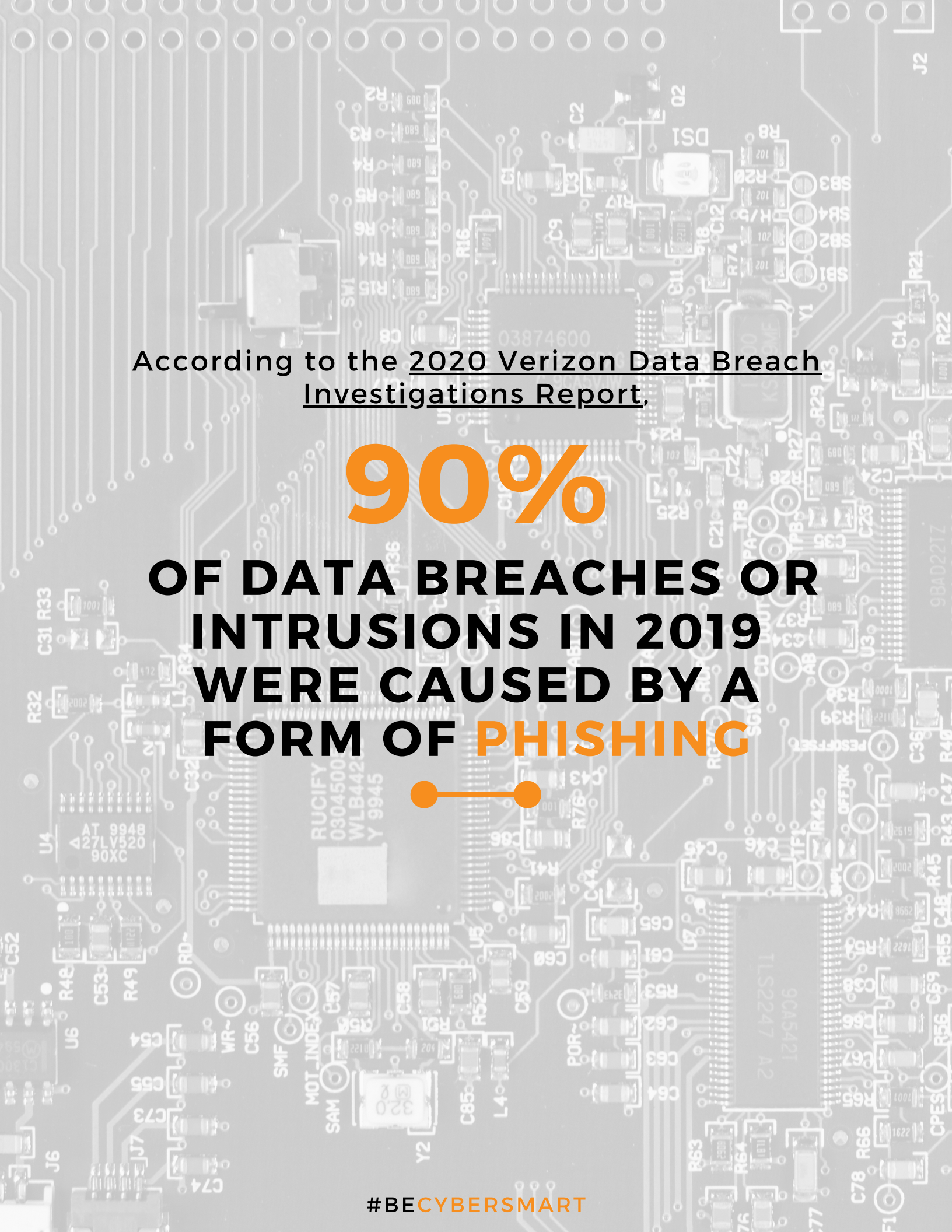
Managing Risk

We connect a lot of devices to a lot of networks. And doing so can put us at risk for exposing our information and data to unknown parties, as well as malware that can steal our data or otherwise compromise our information. As we've mentioned, there are a lot of things we can do to protect ourselves; keeping our security software, Web browser, and OS up to date is critical for protecting our devices from known threats and vulnerabilities.

Be conscious of what you're accessing, where you're accessing it from, and what device you're accessing it with, And remember, if you connect, you must protect.

LEARN MORE

For more information on "Connection Protection": check out this blog post from 'Connected' Magazine



According to the 2020 Verizon Data Breach Investigations Report,

90%

OF DATA BREACHES OR INTRUSIONS IN 2019 WERE CAUSED BY A FORM OF PHISHING

#BECYBERSMART

Let's NOT Go Phishing

There's a reason why Phishing is one of the most common causes of data breaches. A Phishing scam costs next to nothing to employ and has the potential to take down entire organizations. If a Phisher sends out 10,000 e-mails, and just one person takes the bait then the Phisher's campaign is considered a success.

As our daily activities continue to move online, Phishing will become even more of a threat as Phishers hone their email based 'hooks' to better mimic the environment in which they are attempting to Phish.

In response to this threat, the National Institute of Standards and Technology (NIST) has developed a new Phishing Scale that can be used to judge the difficulty a user might have in detecting if a suspicious email is a Phish. NIST hopes that this new Phishing Scale will assist companies in developing improved cybersecurity awareness training that will better equip their employees to detect and report Phishes with a higher degree of accuracy.

CLEVERLY CRAFTED EMAILS

Beyond trying to trick you into clicking on a link or downloading an attachment, Phishing emails must first bypass common Spam filtering. This means that the Phish emails you do see will be much more cleverly crafted than the one caught by the filter.

Both you and your firm need to be aware of the latest trends, tricks, and tactics Phishers will use to 'lure' you in.

TIPS FROM THE CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY (CISA)

Play hard to get with strangers.
Links in email and online posts are often the way cyber criminals compromise your computer. If you're unsure who an email is from—even if the details appear accurate—do not respond, and do not click on any links or attachments found in that email. Be cautious of generic greetings such as "Hello Bank Customer," as these are often signs of phishing attempts. If you are concerned about the legitimacy of an email, call the company directly.

Think before you act.
Be wary of communications that implore you to act immediately. Many Phishing emails attempt to create a sense of urgency, causing the recipient to fear their account or information is in jeopardy. If you receive a suspicious email that appears to be from someone you know, reach out to that person directly on a separate secure platform. If the email comes from an organization but still looks "phishy," reach out to them via customer service to verify the communication.

Protect your personal information.
If people contacting you have key details from your life—your job title, multiple email addresses, full name, and more that you may have published online somewhere—they can attempt a direct spear-phishing attack on you. Cyber criminals can also use social engineering with these details to try to manipulate you into skipping normal security protocols.

TRAIN YOUR PEOPLE TO SPOT PHISHING

It's important for your firm to actively train your employees to spot and report Phishes as they appear. This is why Infoaxis offers **cybersecurity awareness campaigns** to hone your employees' Phish spotting skills. With our help, your employees will not just be another vulnerability for Phishers to exploit, they will be part of the solution your team uses to stop Phishers in their tracks.

Contact Infoaxis to learn more about Cybersecurity Awareness Training

MORE TIPS FROM THE CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY (CISA)

Be wary of hyperlinks.
Avoid clicking on hyperlinks in emails and hover over links to verify authenticity. Also ensure that URLs begin with "https." The "s" indicates encryption is enabled to protect users' information.

Double your login protection.
Enable multi-factor authentication (MFA) to ensure that the only person who has access to your account is you. Use it for email, banking, social media, and any other service that requires logging in. If MFA is an option, enable it by using a trusted mobile device, such as your smartphone, an authenticator app, or a secure token—a small physical device that can hook onto your key ring.

Shake up your password protocol.
According to NIST guidance, you should consider using the longest password or passphrase permissible. Get creative and customize your standard password for different sites, which can prevent cyber criminals from gaining access to these accounts and protect you in the event of a breach. Use password managers to generate and remember different, complex passwords for each of your accounts.

Install and update anti-virus software.
Make sure all of your computers, devices, phones, and tablets are equipped with regularly updated antivirus software, firewalls, email filters, and anti-spyware.

KEY TAKEAWAYS

Cybersecurity may be complex, but its deployment can also be simple.

You need not be a cybersecurity expert to employ good cyber-hygiene and employ basic cybersecurity strategies.

Although we can debate the complexity of cybersecurity, we cannot debate the necessity.

Cybersecurity is no longer a second level consideration. It must be at the top of your priorities list when you connect any device to the internet.

Cybersecurity is for everyone:

You, your colleagues, family, and friends. Everyone who goes online must have a basic knowledge of good cybersecurity practices and hygiene. Thankfully, there are plenty of tools available to help you and everyone you know get started on good cyber practices.

Having experts in your corner can be a huge help.

They have the know-how, experience and resources you need to help keep the bad actors at bay, keep your downtime low, and ensure you can keep your business open and productive.

Worried about Falling Prey to Hackers?

GET A COMPLIMENTARY CUBERSECURITY CONSULTATION

If you are concerned about your organization's cybersecurity, then talk to us. In an initial consultation with Infoaxis experts, you can discover the most critical risks your organization is facing and strategies to mitigate them.

Contact us today – before your organization gets attacked by cybercriminals.

About Infoaxis

Operating in Bergen County, NJ, since 1999, Infoaxis offers managed IT, cybersecurity, and cloud services. We assist large and small healthcare, financial services, law, manufacturing, and construction firms in developing forward-thinking IT strategies and managing their technology assets more effectively. Our cybersecurity team provides critical protection and monitoring to reduce cyber risks, giving clients peace of mind.

We are a privately held company with a long track record of success, including past recognition on Inc. Magazine's list of the fastest growing US companies. Our success is built on understanding our clients and then helping them apply technology solutions to achieve their goals.

INDUSTRY-LEADING MANAGED CYBERSECURITY SERVICES

We help ensure your cybersecurity defenses are in place and deployed effectively against ever-evolving security threats. Our US-based 24/7/365 Security Operations Center can handle your firewall, intrusion monitoring, detection and response, virtual private network, vulnerability scanning, anti-virus, and compliance requirements.

marketing@infoaxis.com
201.236.3000
www.infoaxis.com/services-solutions/cybersecurity

#BECYBERSMART