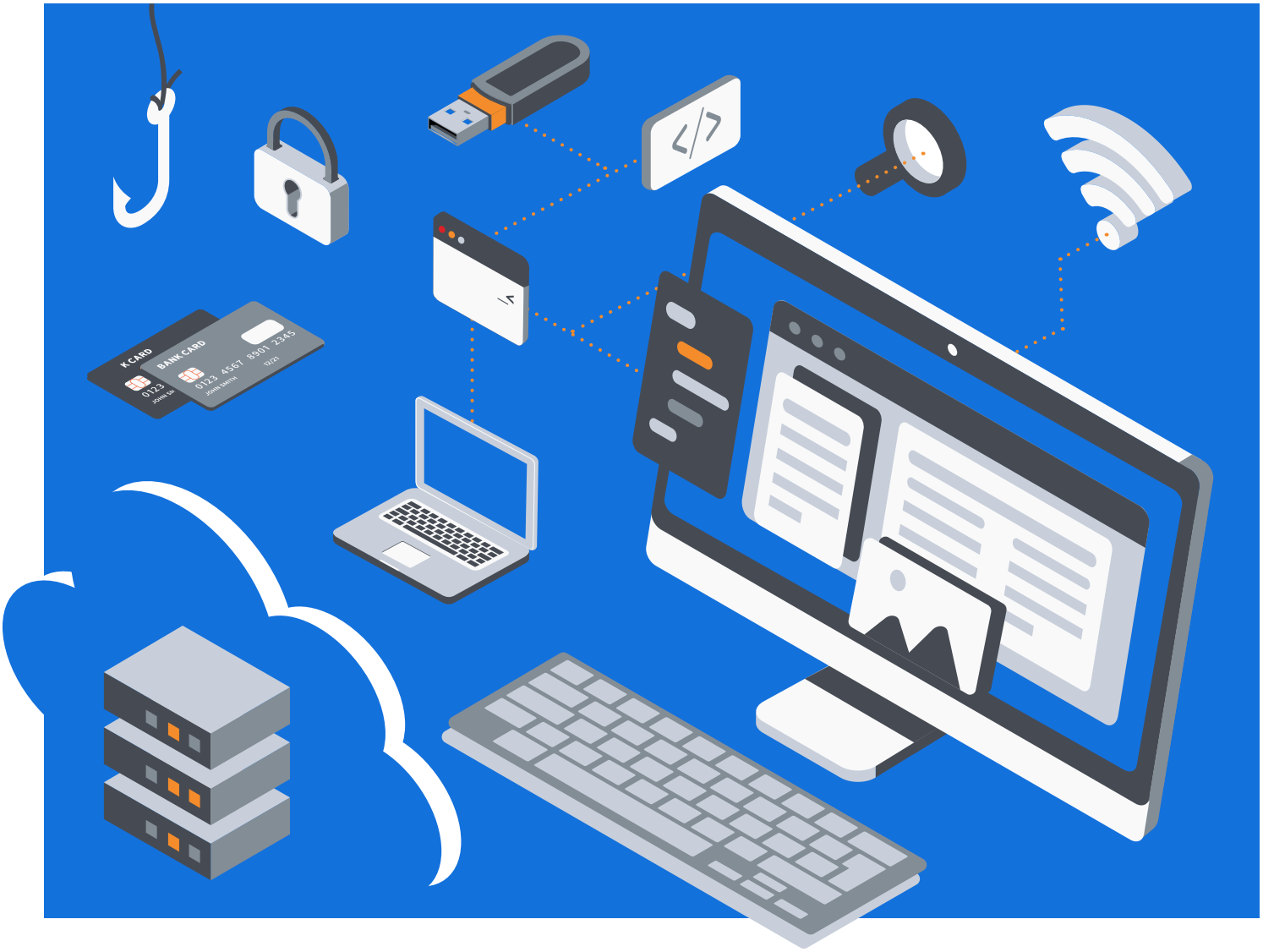
BlackBerry
Intelligent Security. Everywhere.

White Paper



The Zero Trust Guide To Remote Worker Security

Taking a Page from the Zero Trust Playbook for Secure Remote Working

The Zero Trust Playbook

Remote workers need to secure their home network, use applications responsibly, and lock down their devices.

Social Engineering

Ways to Attack	Best Practices
Phishing emails	Pay close attention
Support scam phone calls	Slow down, think
Phony social media profiles	Trust your gut
Bogus notifications	

Wireless Interfaces

Ways to Attack	Best Practices
Cellular network	Disable when not in use
Wi-Fi	"Forget" devices
Bluetooth	Change passwords

Physical Access

Ways to Attack	Best Practices
USB sticks	Never leave unattended
Logged in accounts	Password-enabled screen lock
Bogus notifications	Trust your gut
USB Charging Cables	Use portable chargers

Attack Vector Awareness for Users

With the recent increase in the number of employees working from home as a result of the COVID-19 outbreak, the enterprise network has effectively become much larger, more dispersed, and more difficult to secure.

While organizations can implement Zero Trust strategies and tools to mitigate the additional risk introduced by an expanded mobile workforce, employees themselves can take a page from the Zero Trust playbook by ensuring they practice good cyber hygiene and remain vigilant. The Zero Trust security model trusts nothing and no one by default, and this strategy can be adopted by end-users to increase their security stature.

Remote workers need to take the necessary steps to secure their home network, use applications responsibly, and lock down their devices – both for their own security and for that of the corporate systems they will likely be connecting to a good part of each day.

What happens on the home network can easily bleed over to the enterprise, especially when best practices are not adhered to or applications are employed without understanding how they can impact security both inside the home and inside the corporate firewall.

The Zero Trust security model trusts nothing and no one by default. Under a Zero Trust security model, every user, device, and network are assumed to be hostile until they can be validated, and they are continuously validated to prevent a security lapse. Remote workers can apply the Zero Trust concept of assuming everything is a potential attack or avenue to compromise until they can verify that it is not.

This white paper serves to act as a starting point for remote workers to take some simple steps to improve their security posture when working remotely.

Attack Vector Awareness for Users

Attackers utilize a wide variety of means to infect their targets. Often, attacks leverage one or more of the tactics below, so applying a Zero Trust approach is essential. We'll provide some further details where applicable a little further on in the paper, but first, let's start with some general awareness around attack vectors:

Social Engineering

Social engineering preys upon one of the more difficult vulnerabilities to mitigate: human nature. Social engineering can take many forms, ranging from malicious phishing emails and support scam phone calls to phony social media profiles and bogus notifications from seemly trusted sources. The attackers seek to exploit our innate tendency to trust that if something seems legitimate, it is – however, that is not always the case.

The best advice to reduce the likelihood one falls victim to a social engineering operation is to simply stop and think before acting. Social engineers count on a target being distracted or simply not paying close attention to what they are doing, and often the attacks seek to mimic something routine, like a prompt to click on a link in a parcel delivery notification email, for instance.

Slow down, look for signs something is amiss, trust your gut if it tells you something does not seem right, don't feel pressured to act, and if you're not sure, just stop what you are doing and contact your IT security team for assistance. Social engineering is an aspect of many attacks, so you'll find more risk mitigation guidance where applicable in the sections below.

Physical Access To the Device

An attacker with physical access to an unsecured device can install the malicious software or take control of accounts. This can be done in a number of ways, ranging from the insertion of a removeable storage device like a USB stick, through the installation of malicious programs from an online location, or by accessing accounts to which users are already logged in.

The best advice here is to never leave your device unattended, even for a brief moment, and always ensure you use a password-enabled screen lock with an auto-timeout set, even when you are in trusted environments like the office or at home.

Social engineering can take many forms, ranging from malicious phishing emails and support scam phone calls to phony social media profiles and bogus notifications from seemly trusted sources.

Application Vulnerability Exploits

Vulnerabilities within applications present on a device can be exploited to gain remote access to it. While there is not a lot one can do about unknown or unpatched vulnerabilities, you can ensure that the operating system and every piece of software installed on the device are fully updated.

For the best protection, enable automatic updates for the OS and software so that you don't have to keep track of when new versions are coming out, and you can be confident you'll receive any patches as soon as they are available.

Also, close your apps when not in use. It's less likely an attacker can leverage a vulnerable application if it is not running, and this includes apps that may appear to be closed but are actually running in the background. For mobile devices that are not already equipped, get a good app killer to make sure apps are actually closed when you want them to be. This will also probably improve your battery life significantly.

Note that this is a superficial fix at best. Attackers with enough system privileges can run apps after they have been closed. Later in this paper, we discuss why it is important to create a user profile on your device for everyday use that does not have administrative privileges enabled so that attackers cannot leverage those privileges. Also, ensure devices have a full suite of endpoint protection solutions that can prevent the exploitation of both known and unknown vulnerabilities.

Malicious Apps and Excessive Permissions

Malicious or vulnerable applications downloaded from unverified third-party websites, and even some that are present in legitimate app stores, can be leveraged by attackers to compromise a device. Again, this is a time to stop and think before downloading an application. Crowd-sourced app ratings are a good place to start, but they cannot always be reliable when it comes to judging the security of an application.

Some general security rules-of-thumb: don't jailbreak your devices. If you're not sure what that means, then you don't have to worry about it. Also, check the permissions an application is asking for prior to downloading. Does a flashlight app really need access to your camera, microphone, messaging, and contacts? Probably not.

Again, if you're not sure, just stop what you are doing and contact your IT security team for assistance. Also, make sure your devices have comprehensive endpoint protection installed.

Malicious and Compromised Websites

Infections can occur when visiting websites controlled by attackers. These kinds of attacks are often referred to as "drive-by" or "watering hole" attacks depending on the nature of the operation. Most people understand the risks from casual web surfing and the chance of getting malware infections, but most don't realize that even legitimate sites that have been compromised, or are hosting a malicious ad library, can infect a device.

There are a few things you can do to prevent infection, like making sure your browser is updated to the latest version, installing a legitimate ad blocker program, and just exercising good judgement by not engaging in risky web surfing behaviors. Once again, this is where having a robust endpoint security solution in the device will really payoff.

Infections Via USB Charging Cables

Connecting your mobile device to a compromised charging station or PC with a USB cable could lead to a malware infection. You might think that sometimes you just have to do it, or else you will be without a working device, but that's simply not true – there are better alternatives than relying on risky public charging stations. Personal, portable chargers are inexpensive and easy to keep transport in a backpack or the glove box for your car.

If you find yourself in a position where you don't have one with you, chances are a trusted friend does. Worst case scenario, you will just need to go find an AC outlet and plug directly into it for a bit to get a charge. Note that anytime you are using a USB connection to charge, there is some element of risk because the cable is designed for power and data exchange, but the risk is lower if you're plugging into an AC outlet rather than a USB port. A good endpoint security solution will offer additional protection should the power source be malicious.

Attacks Via Wireless Interfaces

Devices that have wireless interface capabilities can be attacked through cellular network connections, Wi-Fi, Bluetooth, or near-field communications (NFC) – that's just the nature of the risk in any form of connectivity. When not connected but enabled, some of these features scan for connections, and in scanning, they can reveal information about the device that can be leveraged in an attack, so it's good idea to disable them altogether when not in use.

In addition, you will need to change the default passwords and pins for devices connecting via Bluetooth, "forget" devices and Wi-Fi's you are no longer using, and make sure you do not have the auto-connect feature enabled. Also remember, even though NFC connections can only occur over a very short distance, the connection is not secure, so turn it off when not in use.

Finally, it's a good idea to not connect to anything you don't control – the exception might be your good friend's Wi-Fi, but even that has risks if they are not security-savvy and have their network locked down. As is often the case, convenience is the bane of security, and just because a feature is available on a device, that does not mean it's secure to any degree. The best advice here is if you're not using it, turn it off.

Malicious Code

Depending on the type of malware infecting your devices, an attacker may be able to do pretty much anything you can do on your device, and in some instances, a whole lot more. Malicious code such as spyware can record phone calls or other audio like conversations, and record keystrokes to steal information like login credentials. Some spyware can also read text messages and be used to undermine multi-factor authentication.

Remote access trojans (RATs) can let an attacker take full control of your device and modify device settings or take screenshots. RATs can also allow them to impersonate you and potentially infect others in your network. If someone has access to your email, social media, and text apps, they could easily trick your contacts into thinking communications are coming from you.

...you will need to change the default passwords and pins for devices connecting via Bluetooth, "forget" devices and Wi-Fi's you are no longer using...

Malware also presents general privacy concerns, especially if it allows the attacker access to your personal email, text messages, voicemails, content from chat applications, and call logs. Some malware can also allow the retrieval of location data, browsing history, and stored media such as photos and videos, sensitive personal data, and even corporate data if you use your device for work.

Last, but not least, is ransomware. While all malware is bad, ransomware is perhaps the worst of its ilk in some respects. When a device is infected, ransomware will encrypt all the data and then typically produce a message for the device owner with instructions on how they can get a decryption key to restore their data, but this often comes at a significant cost in the form of a ransom demand – hence the name.

It is up to the device owner to decide whether or not to ever pay a ransom to recover data — and there are good arguments for and against doing so and specific risks either way. If you pay, you might not get your data back or it could lead to more payment demands in the future. If you don't pay, you risk losing everything on the device. Obviously, the best mitigation is to not get a ransomware infection at all if possible.

This is where security starts sounding like a broken record because many issues can be addressed with the same proactive approaches, and malware is one of them: keep operating system and software up to date and patched, don't engage in risky online behavior, don't leave devices unattended, and don't click on links or open attached docs in emails without precautions, etc.

When it comes to malware though, the very best measure is to make sure you have a next-gen antivirus running on the device. Why next-gen? Because signature-based antivirus is an outmoded approach that only protects against known threats, not new ones. We'll delve into that a little more below.

Some browsers will even notify the user if the website has a reputation for being risky or malicious. It's a good idea to heed these warnings and avoid those sites.

Improving Web Security

Ways to Attack	Best Practices
Risky Browsing Behavior	Abstain
Media, music and movies torrents	Avoid web torrents
Gambling websites	Avoid risky sites
Shortened URLs	Legitimate URL shortening
Auto-Downloads	Disable All Auto-Downloads

When we say "improving web security" here, we mean protecting yourself and your devices while you're connected to the Internet, doing all the wonderful things you've become so accustomed to doing in cyber space. And once again, this is where security sounds a little repetitive — if you're not using it, turn it off and apply a Zero Trust approach:

Risky Browsing Behavior

One of the easiest things all users can do to significantly reduce the risk of having their devices compromised is to abstain from risky web browsing behaviors. This requires having an awareness of the types of websites that are most often abused in attacks and simply avoiding them when at all possible. While some of the riskiest browsing behavior involving websites of an adult nature probably don't need to be over emphasized here, there are many other types of websites that have high instances of being employed in attacks that users may not be aware of – particularly in regard to keeping the home network secure when working remote.

These sites can include web torrents where users can download media like music and movies, sites often promoted on social media that offer surveys or other novelty gotta-see-this enticements, gambling websites, sites with excessive popups or promoting salacious gossip and news stories, and more. In addition to the vast number of malicious websites out there, users also have to be aware that even legitimate websites can be used to spread malware, including popular gaming websites or news and entertainment sites.

Users should take caution in the sites they choose to browse and ensure they have firewalls enabled on their devices. Users should also ensure that security software is enabled and up to date, and that browsers are also up to date with security features enabled. Users should avoid clicking on popups and trust their intuition – if something doesn't feel right, it probably isn't. The old adage, "if it seems too good to be true, it probably is," also applies here.

One of the easiest things all users can do to significantly reduce the risk of having their devices compromised is to abstain from risky web browsing behaviors.

Disable All Auto-Downloads

To take this a step further and add even more protections when online, you can disable auto-downloads of all media files, such as images, audio, video, and document files, in applications and browsers. Anytime you have a feature set to automatically do something that involves the transfer of data, you are at greater risk. Again, convenience is the bane of security.

Even though it's nice to scroll through social media feeds and click on all the interesting content, you have to know it can put you in jeopardy. Now, you might be willing to accept the additional risk, but if you use the device for work, you have to realize that you are also putting the company at risk. It's best to consult your organization's security policies to make sure you are in compliance, and if there is something you don't understand, simply ask your security team to explain.

Checking Shortened URLs and Documents

Shortened URLs, which are particularly popular on social media sites like Twitter that have character limits, present a potential problem for users because they do not readily show exactly to where the link is directing. In addition, custom URL shorteners used in creating branded vanity links can also be used to create links that look like legitimate, full-length URLs that are actually directing to a malicious website. While the majority of shortened URLs are probably not malicious, users need to take some precautions to make sure they don't click on one that is.

Often, you can see the destination path for a shortened URL simply by hovering the mouse curser over it before clicking. Legitimate URL shortening tools usually offer a way to unshorten URLs created with their tools, and there are also a number of other URL unshortening sites available. We suggest consulting your organization's security team for recommendations on which to use, or do some careful investigation yourself before choosing one.

There are also free tools available that can check a URL against antivirus scanner data to reveal if the website is malicious and serving up malware. Some of these services also allow the uploading of files and documents that can be scanned as well to determine if they may be tainted.

Again, consult with your organization's security for recommendations on the use of these tools before engaging, and be aware that submitting documents to these tools for analysis means you could be violating company policy, confidentiality agreements, or regulatory requirements about how data is handled, so be sure to get expert advice first. An endpoint security solution will also help protect you against attacks via malicious or spoofed URLs.

There are free tools available that can check a URL against antivirus scanner data to reveal if the website is malicious and serving up malware.

SSL/HTTPS and Website Security

It used to be the case that only some websites adhered to security best practices by offering encrypted connections, such as banking and ecommerce sites where sensitive information is being exchanged. Today, those best practices should be in place for any and every website regardless of whether sensitive information is involved simply because it protects users from attacks.

When visiting any website, especially those noted above where sensitive information exchange is involved, users should make sure they see “HTTPS” and/or the lock icon in the URL address bar to ensure the website is encrypting all of the traffic by way of Secure Socket Layer (SSL). SSL ensures that the connection between the server and the client is encrypted.

In short, there is really no good reason for a website to not be encrypting the entire session regardless of the activity the user is engaging in, and if the site does not offer this basic level of security, it’s a good idea to not engage with it. On occasion, a user will run into a warning that a security certificate is expired for a website, and this is another good reason not to engage with it. The most popular browsers in use will typically warn users if a website is insecure.

Some browsers will even notify the user if the website has a reputation for being risky or malicious. It’s a good idea to heed these warnings and avoid those sites. There are also tools and services available that provide DNS filtering that blocks unsafe websites automatically. Ask your organization’s security team for recommendations on DNS filtering options but be aware it may block sites you or your family are accustomed to frequenting due to their history of being abused, as noted in the Risky Browsing Behavior section above.

...there is really no good reason for a website to not be encrypting the entire session regardless of the activity the user is engaging in, and if the site does not offer this basic level of security, it’s a good idea to not engage with it.

Email Security and Awareness

Ways to Attack
Phishing and Spear Phishing

Best Practices
Don't click links
Don't open untrusted attachments
Disable automatic download of images
Don't open unsolicited email from anyone you don't know
Be aware of spelling and grammatical mistakes

Email is one of the leading attack vectors, and we can't emphasize enough how important it is to be vigilant when it comes to email security — again this is where a Zero Trust mentality is critical. As end-users, we have become too accustomed to using email for routine and often voluminous levels of communication, so it's easy for us to drop our guard, and this is what attackers count on to be successful.

Phishing and Spear Phishing

Most of us are probably cognizant of the risks from spam emails that can be part of phishing campaigns. In brief, phishing is a form of social engineering (covered above) where attackers attempt to trick recipients into revealing sensitive information or executing malware and infecting their device and connected network, and more.

Spear phishing takes phishing to another level by leveraging privileged or specific information related to the target that significantly increases the likelihood the attack will be successful. This can also include the use of spoofed emails that are crafted to appear to be from a legitimate and trusted sender, and even the compromise of personal or corporate email accounts used in an attack, where the email is ostensibly actually from a trusted source.

Phishing emails can include malicious links or tainted documents that can lead to malware infection, or may just contain instructions to navigate to a website that seems legitimate but is controlled by the attackers where the target is asked to enter account credentials or other sensitive information.

How Do I Protect Myself from Email Attacks?

The following are some guidelines for protecting yourself from common email attacks. Please note that this is not an exhaustive list by any means, and every user would benefit from more detailed security awareness training. Ask your organization's security team what resources are available. Also, as with all things security, slow down and think before acting.

Review the email sender — some phishing email have come from attackers posing as legitimate senders using URLs that are similar to the real entities, such as "cdc-gov.org", rather than "cdc.gov". It is best to treat all emails as potentially malicious and exercise caution — remember that even legitimate email addresses can be compromised.

- **Don't click links:** Hovering your curser over links can show you the address they lead to, but it is a best practice to only type trusted URLs directly into a browser, and to never click on links in emails, even if the email appears to be from a trusted source.
- **Don't open untrusted attachments:** Be careful with attachments, especially if you don't recognize the sender or the email appears suspicious. Make sure you are running an endpoint protection solution that can protect you from malicious attachments should you encounter one.
- **Disable automatic download of images:** They can contain malicious code and infect a device simply by opening the email. It is best to only download images from a confirmed and trusted source.
- **Don't open unsolicited email from anyone you don't know:** It is best to send these emails to your spam folder and not risk compromise – rarely would any important communications come from an unknown source through an unsolicited email.
- **Be aware of spelling and grammatical mistakes:** These can be red flags for scams and email-based attacks. Also be wary of generic greetings, such as "Dear Sir" or greetings that seem overly personal such as "Dear Beloved" – these are also likely indicators of malicious intent.
- **Avoid email that demands immediate action or requests for your personal information, passwords, or login credentials:** Attackers will often try to instill a sense of urgency in their targets so bad decisions are made.

Ask your organization what tools it can provide to ensure the security of your email and how to use them effectively to protect yourself and your company. A robust endpoint security solution should be top of the list.

Ask your organization what tools it can provide to ensure the security of your email and how to use them effectively to protect yourself and your company. A robust endpoint security solution should be top of the list.

Home Network Security

Ways to Attack	Best Practices
Home Wi-Fi Router Security Modem Security	• Change default password • Update firmware • Enable automatic updates if possible

While setting up home networks is relatively simple, ensuring those networks are secure actually takes more than a few steps on the part of users. Ensuring home networks are properly secured is critical not only to protect users from attacks, but also from allowing attacks to pivot to corporate networks, a risk that has increased significantly with the surge in remote workers.

This section covers a few of the key items that need to be addressed to secure a home network from a Zero Trust perspective, but again, this is not an exhaustive set of guidelines. Users, especially those who are working from home and connecting to corporate networks, should consult their organization's security team for a complete set of guidelines and protocols to adhere to security and device use policies. You should also take care to follow some of the other best practices outlined in this guide to reduce the risk of falling victim to attacks:

Home Wi-Fi Router Security

For the most part, setting up home Wi-Fi routers is a simple out-of-the-box, plug-and-play process, and often, setup is performed by the user's internet service provider (ISP). Chances are though, that not all of the steps required to secure the router have been followed, so it's good to double check that the following has been done:

First, be sure to change the default administrator password for the router, because these devices are typically shipped with the same password for every device manufactured, and make sure to give your network a unique SSID name. Also make sure the device is updated with the latest version and enable automatic updates if you have the option – otherwise, you need to set a reminder to check if updates are available periodically.

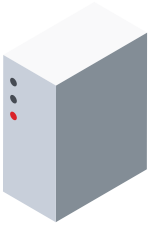
It's also a good idea to change the default passwords for any and every device connecting to the router, such as smart TVs, printers, and other Internet-enabled connected devices in the home. If a device's setup involves connecting to the Wi-Fi, chances are it has a default password that needs to be changed. Also, turn off Universal Plug and Play (UPnP) on all connected devices. While this is a convenient feature for all connected devices on the network to discover one another, it also makes them vulnerable to an unwanted device connecting when in range of the home network.

For the Wi-Fi router itself, it is important that the connections be encrypted to make them, and the data being shared, more secure and private. Be sure to use the WPA2 or WPA3 encryption standards because they provide much better security than WEP or WPA can provide. If you can't figure out how to do this, your ISP technical assistance, or tech assistance at the store you purchased the device if it was not supplied by your ISP, can help you.

Also enable MAC address filtering for an added layer of protection. All devices have a unique MAC address assigned to them, and MAC address filtering prevents devices you have not approved from connecting to the network. And make sure your router's firewall is enabled and configured properly. While your Mac or PC will have a firewall built-in, other smart devices connected to the home network probably do not, so the wireless router firewall is an important layer of defense so you don't wake up one day to find your smart refrigerator is part of a botnet engaged in a denial of service attack or massive spamming operation.

Modem Security

All home network Wi-Fi traffic goes through the router, but if your ISP also requires a modem – as is the case with most cable companies who also provide Internet – you might not realize that most of that traffic is then routed through the modem, so it needs to be secure as well. How to do this will vary with every manufacturer, and sometimes also across models from the same manufacturer, but generally, you will want to do the same things you did with the router, minus the encryption steps. Namely, change the default password, update the firmware, and enable automatic updates if possible. The setup instructions should have steps for security, or you may need to contact your ISP for details.



It's a good idea to change the default passwords for any and every device connecting to the router, such as smart TVs, printers, and other Internet-enabled connected devices.

Device and Account Security

Ways to Attack	Best Practices
Device Security	• Never leave your device unattended • Enable auto-timeouts • Strong passwords • choose multi-factor authentication (MFA) • Password managers • Disable Wi-Fi, Bluetooth, and NFC when not in use • Make sure all devices that can run a next-gen antivirus solution

A central theme running through this guide is that users need to take precautions in regard to what activities they engage in on their devices to reduce the risk of falling victim to an attack – a key strategy in applying a Zero Trust mode of thinking. That said, simple human nature ranging from curiosity to carelessness is a significant factor in our susceptibility to attacks, so it's important to make sure users adhere to some best practices and take advantage of features and tools designed to mitigate some of those risks to devices and accounts. The following are some steps you can take to ensure your devices remain secure:

Device Security

Never leave your device unattended and always have a screen lock feature enabled that requires a pin or passcode to access the device. It is also a good idea to enable auto-timeouts that will lock the device when not in use for a short period of time in case you forget to lock the device if you get distracted with another task.

In addition to strong passwords for account access, be sure to choose multi-factor authentication (MFA) options whenever available. While MFA combined with strong passwords does not provide absolute security, it does significantly reduce the risk of unauthorized use.

Password managers may be a good alternative because they allow users to secure accounts with hard to guess and strong passwords, but only require the user to remember one. For that one password, a long and strong passphrase (32 characters or more) with a combination of upper and lowercase letters, numbers, and special characters is recommended. Password managers typically offer MFA, which is also highly recommended. Never reuse passwords, and never share them for any reason.

For devices like laptops and desktops, it is recommended that users set up two user profiles, one that does not have administrative privileges for everyday use, and one that does for limited circumstances where it is required for device or software maintenance tasks. Using a device with a profile that does not have the elevated privileges reduces the likelihood that an attacker can take full control of a device.

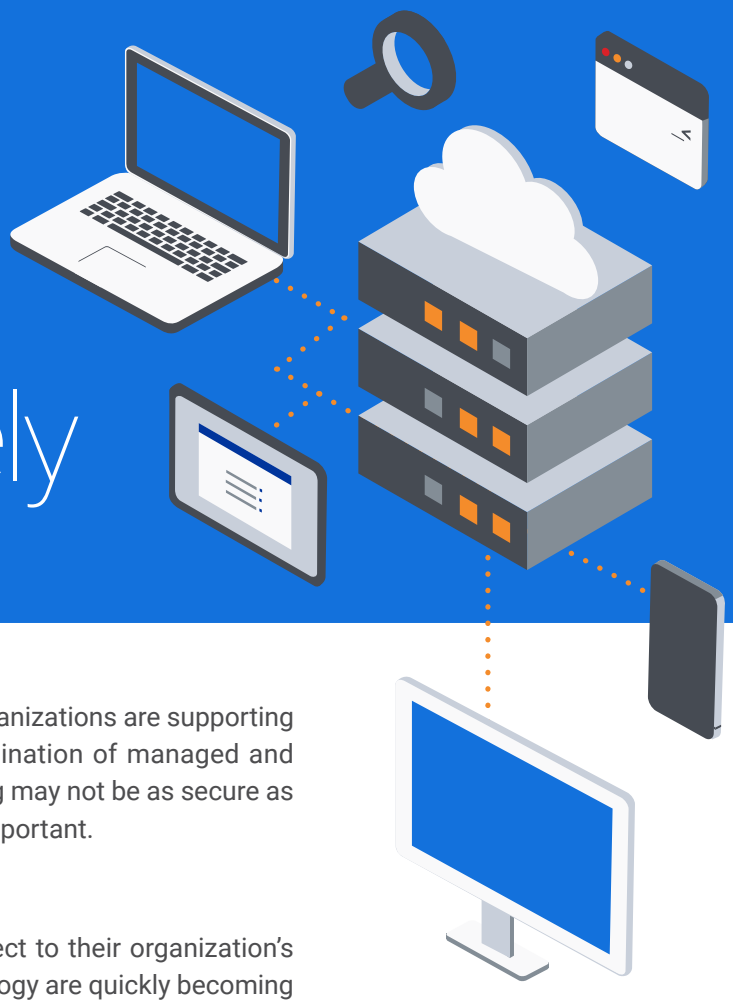
As discussed in an earlier section of this guide, users should disable Wi-Fi, Bluetooth, and NFC when not in use and log out of third-party apps, especially when traveling. When possible, uninstall third-party apps that are not required for the duration of the trip. It is also highly recommended that users install whole disk encryption on devices they travel with, which will protect sensitive data in case the device is lost or stolen.

Ensure devices have the latest operating system and software updates and enable automatic updates if possible. Do not add unknown contacts to third-party apps or click on unsolicited links in email – always enter a URL directly into a browser to assure you are directed to the desired website. Also, do not use personally installed or third-party applications for any corporate communications or file-sharing – consult your organization for approved collaboration and communications software.

Make sure all devices that can run a next-gen antivirus solution have one installed and updated. Next-gen solutions provide more comprehensive protection than outmoded signature-based antivirus offerings that can only protect against known attacks. Also ensure your device has automatic backup and recovery for important files in case your device gets infected with ransomware. Backups are also important if the device is lost or stolen, and features to allow device location and remote wiping of data from lost devices provide an extra level of data loss protection.

Using a device with a profile that does not have the elevated privileges reduces the likelihood that an attacker can take full control of a device.

Connecting To the Corporate Network Securely



Connecting to the corporate network securely is critical when organizations are supporting a large, distributed workforce who may be working on a combination of managed and unmanaged (BYO) devices, and traditional methods of connecting may not be as secure as assumed. Again, taking a cue from the Zero Trust approach is important.

VPN Risks

While VPNs are a convenient, easy way for employees to connect to their organization's network, the drawbacks due to security limitations of this technology are quickly becoming more apparent. Vulnerabilities such as IPv6 leakage due to outdated tunneling protocols where the traffic is routed through IPV4 connections, increased resource requirements to support complicated VPN distributions, patching issues, and the lack of multi-factor authentication use can increase the risks for the organizations that depend on VPNs for connectivity.

In addition, the use of VPNs for BYO devices is generally a bad idea. Even with good identity and access management and use of multi-factor authentication, connecting to corporate systems by way of VPNs allows a significant level of access to the entire enterprise network and introduces risk. Even if the VPN connection is secure, an infected device can be used as a pivot to infect an organization's internal systems. VPNs can also reduce productivity due to significant performance issues for employees working remotely who are using consumer-grade Internet with lower bandwidth

Secure Internet Gateway

A secure Internet gateway is a viable alternate solution to VPNs because it can provide secure access from anywhere to any application, desktop tool, or file on a corporate network. Remote workers can use managed or personal devices to access behind-the-firewall content without sacrificing the performance they enjoy when working in a traditional corporate-owned and managed environment.

These browser-based, containerized solutions also offer secure and auditable aggregation of enterprise assets in a single virtual desktop environment and provide access to all enterprise apps, tools, and files, even when working offline in the case of intermittent connectivity. They also provide turnkey access management to quickly onboard or offboard users and provision endpoints more easily than VPNs.

While VPNs are a convenient, easy way for employees to connect to their organization's network, the drawbacks due to security limitations of this technology are quickly becoming more apparent.

Security Awareness and Incident Reporting

Supporting remote workers securely will require organizations to provide continuous security awareness training as well as a clearly delineated security incident reporting and response capability as part of a Zero Trust strategy:

Security Awareness Training

Organizations should engage in ongoing security awareness training for employees regardless of whether they are working within the corporate environment or remotely. Continuous security awareness programs should work to both educate employees on security best practices as well as provide organizations with auditable feedback on how the program is performing. There are a wide number of organizations that offer security awareness training programs, some at no cost.

All employees, contractors, interns, and partners who interact with the enterprise network should review security protocols and be familiar with them and adhere to the controls required to assure secure remote work. Keep a security-first mindset, as with any security or safety risk, the best approach is prevention. Every employee should recognize they are the frontline for their organization's security team.

Incident Reporting

Organizations should provide clearly outlined steps for employees to take to decrease the potential damage from a suspected security event and report the event to the right teams within the company. Employees, especially those working remotely who do not have immediate access to security teams, will need to have the ability to report a suspected security event that is not reliant on using any device that may be compromised.

Continuous security awareness programs should work to both educate employees on security best practices...

Conclusion

With the likelihood that work-from-home will be a significant aspect of the new normal, even after the COVID-19 crisis subsides, employees will need to ensure they practice good cybersecurity hygiene and remain vigilant and aware. This is where applying a Zero Trust approach to everything they do is advantageous to good security practices. Team members will need to secure their home networks, use applications responsibly, and lock down their devices for their own security, and for the security of corporate networks, because what happens on the home network can easily bleed over to the enterprise.

As organizations continue to work to provide access to enterprise networks for remote workers during the COVID-19 crisis and beyond, they'll need to assure their mobility solutions offer the highest level of security based on a Zero Trust framework where user access is concerned, as well as provide the training and support employees require to remain secure. The whole process needs to be manageable for IT administrators and employees because with a potential flood of new remote users, solutions need to provide simple onboarding and offboarding of users, devices, and applications.

As always, the BlackBerry team is here to help and would be happy to discuss options for securely enabling a remote workforce. You can also reference our white paper, *Seven Strategies to Securely Enable Remote Workers*, which examines Zero Trust strategies to assure effective security controls are in place to govern every user, device, application, and system interacting with an organization's IT environment and beyond.

About BlackBerry

BlackBerry (NYSE: BB; TSX: BB) provides intelligent security software and services to enterprises and governments around the world. The company secures more than 500M endpoints including 150M cars on the road today. Based in Waterloo, Ontario, the company leverages AI and machine learning to deliver innovative solutions in the areas of cybersecurity, safety and data privacy solutions, and is a leader in the areas of endpoint security management, encryption, and embedded systems. BlackBerry's vision is clear — to secure a connected future you can trust.

For more information, visit BlackBerry.com and follow @BlackBerry.

BlackBerry
Intelligent Security. Everywhere.

BB20-0236 | 200520