OPTIV

What to Do When Everything Changes

ISSUED: JUNE 2020

CYBERSECURITY #1 FIELD GUIDE

Table of Contents

01

How to Use This Guide

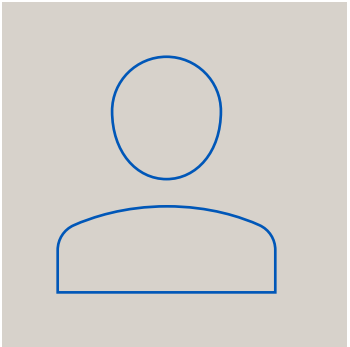
This field guide has been uniquely designed to help you navigate the complex world of cybersecurity.

With the environment constantly changing due to new innovations and threats - including pandemics - this guide starts by helping you assess where you stand as an organization. From there, we'll outline how to identify common threats as well as tools and strategies to prevent them.

In closing, we'll take a look at what's on the horizon including remote work and talent demands.

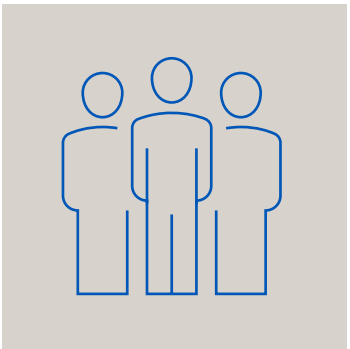
Category Icons

In an effort to make certain types of information easier to find, the main entries in this field guide are designated with category icons for the relevant audience.



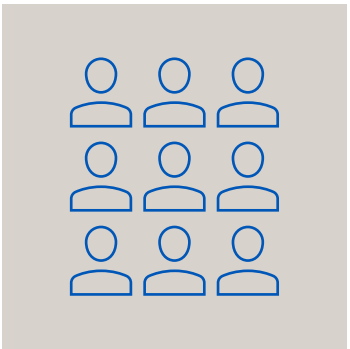
Self

Entries with this icon have information relevant to individuals and may be helpful in professional and personal contexts.



Team

Used with entries that are helpful to small- to mid-size teams.



Organization

These entries provide actionable steps that go toward securing the entire organization.

02

Assessing the Situation

Effective security reflects a deep understanding of your environment. During significant bouts of industrial change, thoroughly assessing the impact on your business can help maintain continuity while mitigating unexpected consequences. In this section, we explore methods of forecasting change and maintaining continuity in the face of major environmental change brought on by a pandemic.

Maintaining Business Continuity

Choosing the most effective cybersecurity strategies to ensure business continuity is paramount to endure a crisis and mitigate risk. Employing proven strategies – like expanding what you currently have, creating alternative access methods and redesigning your cybersecurity program at scale – can replace uncertainty with confidence. These approaches, and the actionable technical steps below, provide the foundational support needed to enable and secure a work from home (WFH) model.

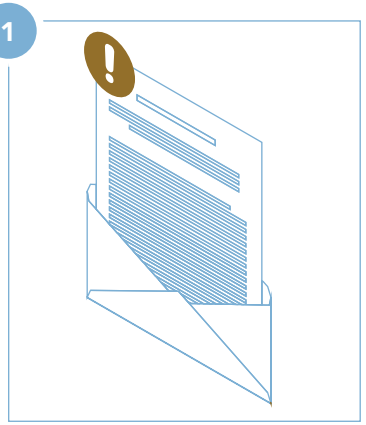
In all of these solutions, ensure that proper validation and testing of security solutions is taken into account. Attack surface management and penetration testing for validation ensures the guidance put in place reduces risk to you and your WFH employees.

Adopt a Flexible Mindset

- Shorten the normal testing cycle and change management to match production changes
- Provide the best level of risk assurance possible given current conditions
- Clearly explain the threats and risks that the organization might encounter
- Consider your response plan to adapt to all changes in circumstance

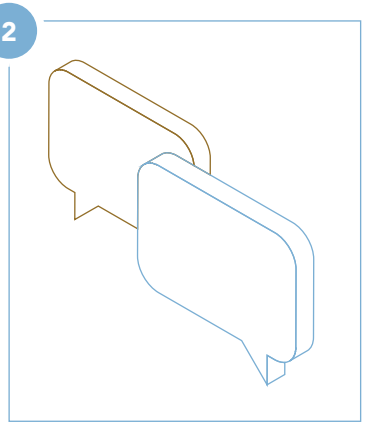
Crisis Business Continuity Steps

1



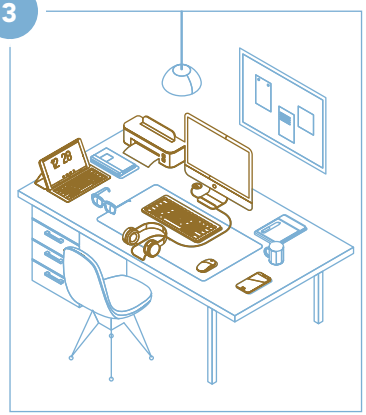
Establish crisis communication expectations and create an email alias so users can easily identify "official" corporate communications related to how the virus is affecting the company and their employees.

2



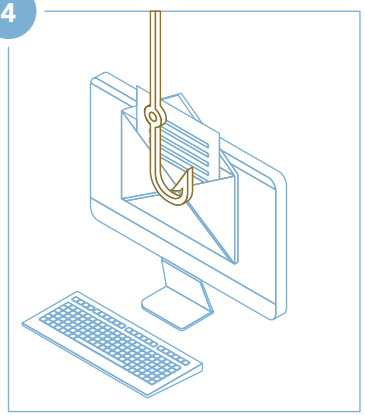
Provide a feedback loop for the remote user experience and act on valid feedback quickly to reduce Shadow IT solutions to remote user problems.

3



Provide employees with guidance on WFH best practices like setting aside a dedicated workspace, adhering to a schedule etc.

4



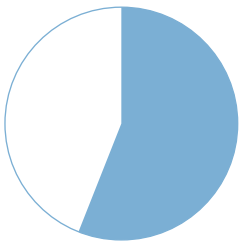
Be aware of disinformation campaigns around the crisis.

Work from Home Forecast Post-COVID-19

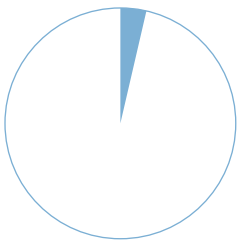
We predict that the longer working from home is mandated, the more widespread its adoption will be when the dust settles.

Studying the Trends

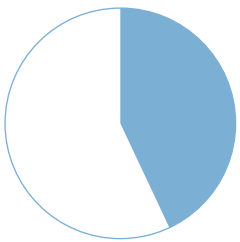
Based on historical trends, we expect that those who worked remotely part-time before the pandemic will increase their remote work frequency after they're allowed to return to the office. For those who were new to remote work until the pandemic, we believe there will be a significant upswing in their adoption. Our best estimate is that we will see 25-30% of the workforce working at home multiple days a week by the end of 2021.



56% of the U.S. workforce holds a job that is compatible (at least partially) with remote work

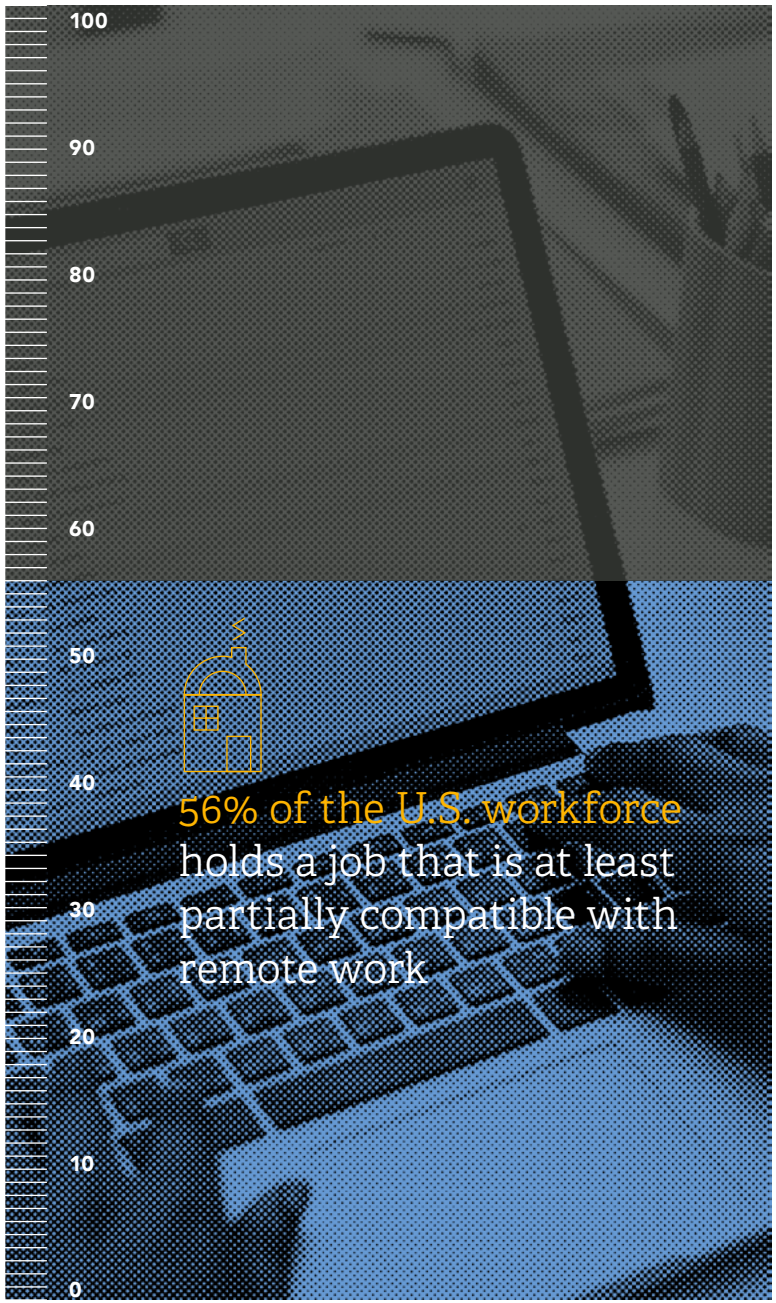


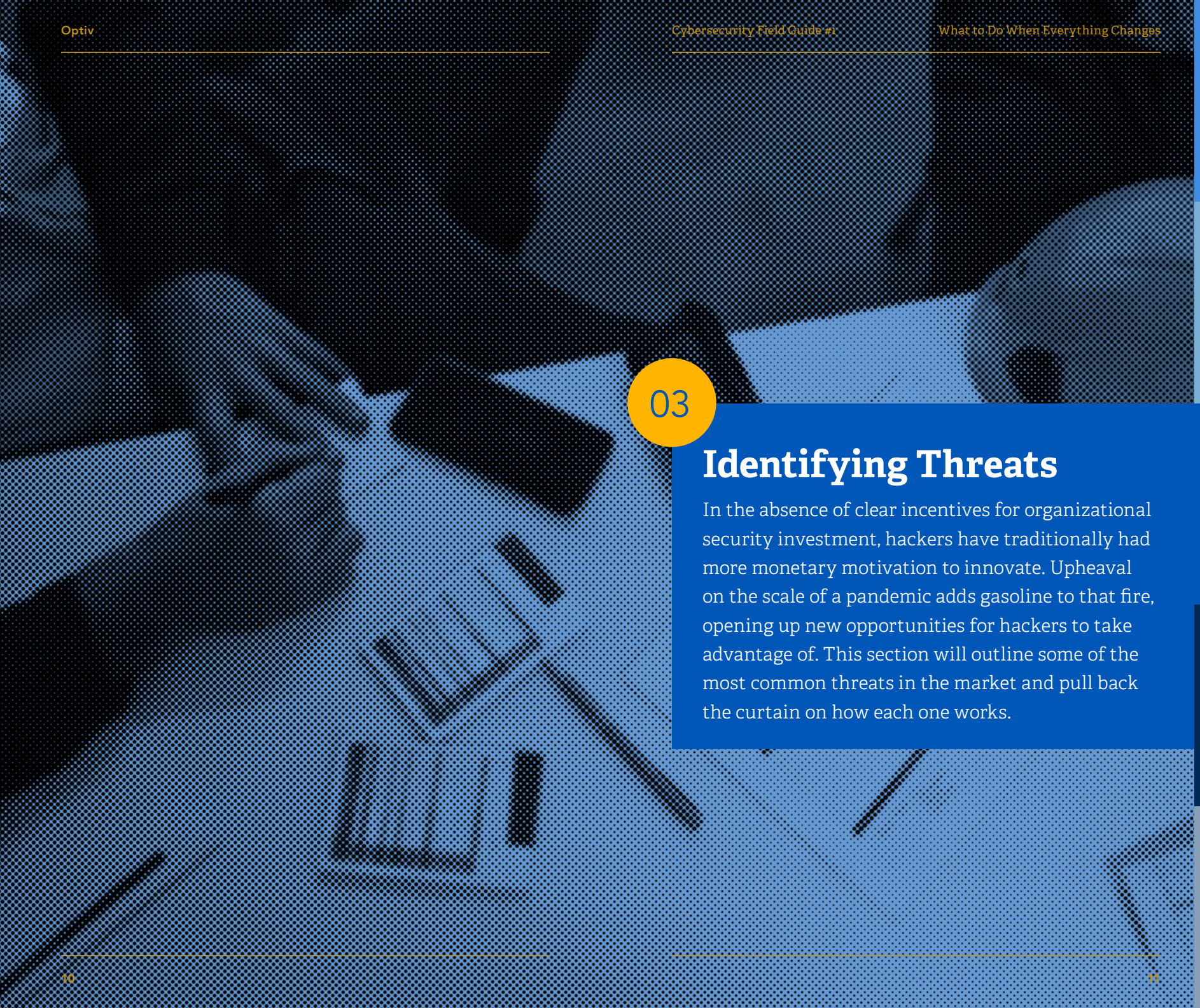
Before COVID-19, only **3.6% of the employee workforce** worked at home half-time or more



Gallup data from 2016 shows that **43% of the workforce** works at home at least some of the time

Source:
Global Workplace Analytics, 2020





03

Identifying Threats

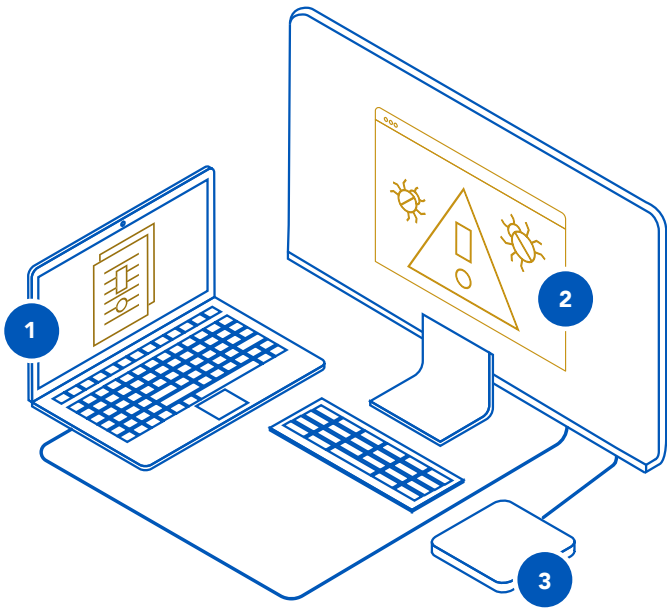
In the absence of clear incentives for organizational security investment, hackers have traditionally had more monetary motivation to innovate. Upheaval on the scale of a pandemic adds gasoline to that fire, opening up new opportunities for hackers to take advantage of. This section will outline some of the most common threats in the market and pull back the curtain on how each one works.

Malware

Malware is malicious software that is intended to gain access to, damage or disable your device. It can compromise your security, gain remote control of your computer, cause financial loss and destroy data.

Common ways malware can be unknowingly installed:

1. Visiting malicious websites
2. Clicking links or opening attachments in phishing emails
3. Plugging infected external devices into your computer



94% of malware is delivered via email, with an infected Word doc or attachment making up 45% of those malicious emails.

Verizon DBIR, 2019

Falling for phishing emails and **visiting malicious websites** are the two most common ways that malware is distributed to users.

Once malware infects your computer, cybercriminals can obtain your financial and personal information, spy on your computer activity and compromise your data by holding it ransom. **Malware is capable of taking down entire company networks.** By utilizing the computing resources within the company, the malware disrupts traffic and overloads servers resulting in an internal Distributed Denial-of-Service attack (DDoS).

Malware can infiltrate your devices in many ways.

Be mindful that outdated software and operating systems have less sophisticated security defenses and are more vulnerable to malware infection.

Keeping software and operating systems up-to-date is an important part of ensuring security.

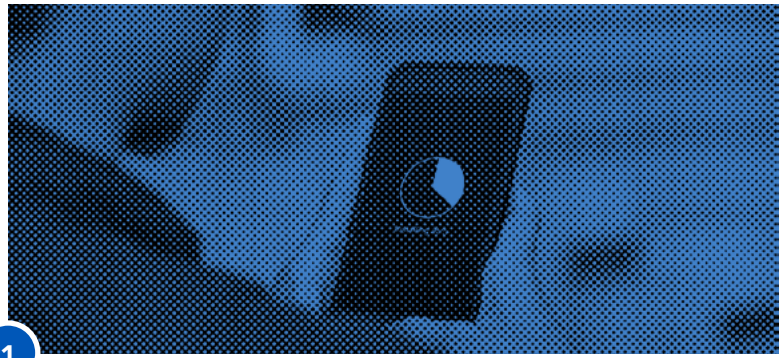
Common attack vectors for malware include:

- Links or attachments in phishing emails
- Malicious websites
- Malicious apps, plug-ins or programs
- Unsecured WiFi networks
- Infected external drives
- Exploiting security vulnerabilities in outdated software or hardware

Malware Signs of Infection

Despite best efforts, sometimes malware sneaks into our devices. Learning what to look for will help you avoid it, but will not always prevent infection.

Sure signs that your device is infected include:

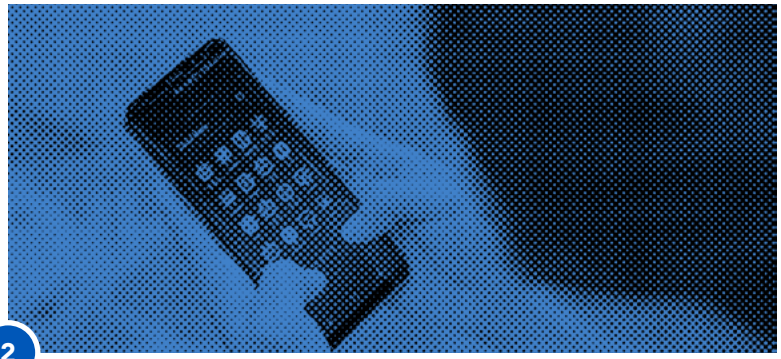


1

Slowdowns

Your device is chugging at unusually slow speeds or frequently freezes, restarts or crashes. Programs or apps behave uncharacteristically, opening and closing automatically or consistently do not respond. Your device is suddenly running low on memory or out of free space on its hard disk.

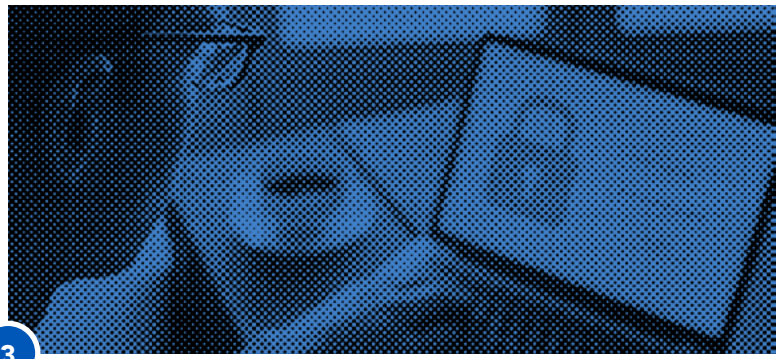
If you suspect that your device has been infected by malware, contact technical support immediately.



2

"I didn't do that..."

Strange files, suspicious software or mysterious apps appear on your device. Sometimes your web browser's home page may change without any action from you. Emails propagate in your sent folder or you receive multiple delivery failure notices for messages you did not send. Your contacts report strange emails, calls or texts from you. You may even receive alerts about unexplained data overages or purchases you did not authorize.



3

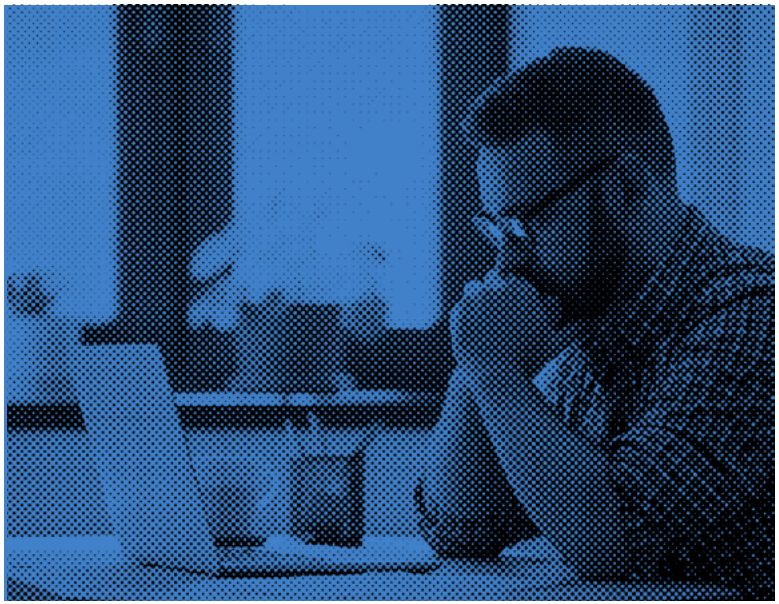
Out of control

Your passwords have been changed, leaving you unable to log in to your device or network. Your device's operating system refuses to shut down or prevents access to its task manager or activity monitor. Your web camera turns on, your anti-virus is disabled or your browser redirects to websites without permission or intervention.

Ransomware

Ransomware poses a major security threat to individuals and organizations. Cybercriminals have used ransomware to seize control of organizations' systems, steal data and shut down healthcare providers, public transportation and higher education institutions in at least 150 countries.

Risks associated with crypto ransomware can include intellectual property loss, harm to the organization's ability to operate and more. Associated financial losses are difficult to pinpoint, but are estimated to be in the billions of dollars.



Locker vs. Crypto Ransomware

Locker ransomware is an older, less-sophisticated form of ransomware. As the name suggests, it locks the entire device on a ransom message screen, denying access until a fee is paid. It typically does not encrypt files and leaves the underlying system largely untouched, making it easier to remove. Locker ransomware often poses as law enforcement agencies to make the victim believe legal action will be taken for purported criminal activity.

Crypto ransomware is a sophisticated form of ransomware that can cause serious damage, often before it's noticed. Once installed, crypto ransomware leaves the device operating normally as it infiltrates the system undetected. After it encrypts files (a process where the data is transformed into a code that requires a key to decipher), the victim is presented with a demand for payment. It is incredibly difficult to remove this type of ransomware and may lead to permanent data loss.

Ransomware Targets

Personal Computers

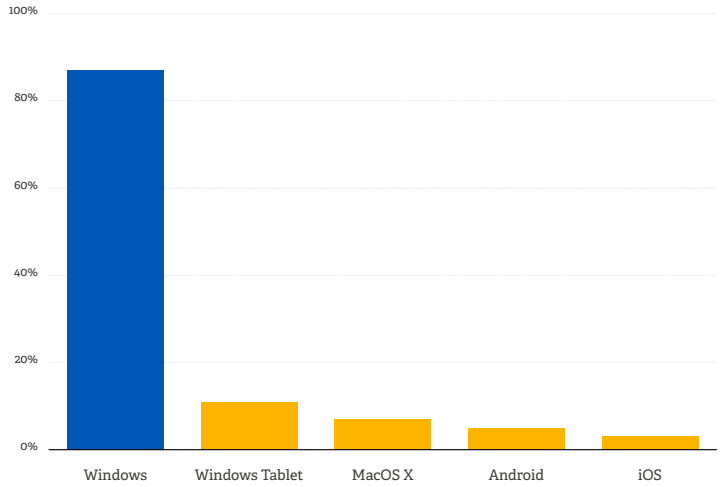
Personal computers are typically targeted through phishing emails. Ransomware must be tailored to the targeted operating system (OS) to leverage the computer's programming to block or limit access to system files. Ransomware is not typically cross-platform between Windows and Mac.

Mobile Devices

Locker ransomware favors mobile platforms because mobile devices are less likely to store sensitive files that would otherwise be exploited by crypto ransomware.

Avoid downloading third-party apps from unofficial sources. Always examine the publisher, read user reviews and review the permissions that the app requests.

Major Operating Systems Targeted by Ransomware According to MSPs 2019



Source: Worldwide; Datto ; 2019; 1,400 respondents; managed services providers

Company Servers

Ransomware may attack servers to shut down operations and demand payment. It can be used as a smokescreen for other nefarious activity resulting in a breach of private files and customer data. Legal implications can result in heavy financial loss and severe damage to the company's reputation.

IoT/Other

While not yet as prevalent, ransomware could be deployed on other devices such as smart home appliances, voice-activated assistants, smart watches and WiFi surveillance cameras. As technology progresses, Linux-based systems are being implemented in small gadgets and smart home objects that have the potential to be targeted by ransomware criminals.

Identifying Other Threats

In the absence of clear incentives for organizations to invest in advanced security resources, hackers have traditionally had more monetary motivation to innovate. Hackers usually have more motivation than organizations to innovate their methods and pandemic events open up even more opportunities that hackers can take advantage of. This section will outline some of the rising threat tactics in the market.

1 Vishing

Vishing is the use of voice calls or messages from criminals claiming to be from a reputable company. The caller may use scare tactics to compel an individual to reveal personal details or banking information.

2 Malicious Apps

Malicious apps remain the most common means of infecting mobile devices. These apps have been found on both third-party and official app stores. Once installed, malicious apps can authorize fraudulent charges, steal login credentials, extract data or add the device to the cybercriminal's botnet.

3 Malicious Sites and Adware

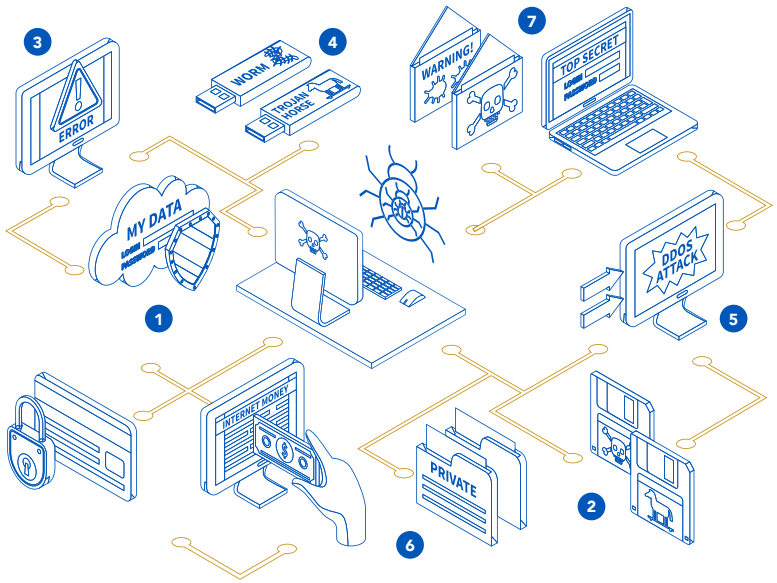
Malicious sites or adware can trigger the installation of malware onto your device if you are using an Android device that allows for file management.

4 Physical Installation

Physical installation of malware can occur if a cybercriminal steals your device and installs malware by plugging it into a hacking device. This is often a targeted attack. Phones that are sold by a third party are sometimes already infected in this manner prior to purchase.

5 Outdated Software

Using outdated software may expose you to security flaws that hackers are able to easily exploit. As an example, older Bluetooth technologies were able to be hacked via Bluetooth without the user connecting or authorizing access.



6 Unsecured WiFi

Each year, mobile threats are increasing both in number and severity. Using free, unsecured WiFi networks on your devices can be tempting, but be aware that once connected, cybercriminals could be watching your every move.

7 Mobile Malware

Malicious applications don't just appear in third-party app stores.

In 2016, KeyRaider, an iOS malware that was capable of making unauthorized in-app purchases and stealing usernames and passwords from Apple iCloud users, successfully snuck into the App Store.

Around the same time in the Google Play Store, hundreds of well disguised malicious apps with the DressCode trojan infected Android devices to use them in a botnet for DDoS attacks, spam emails and cryptocurrency mining. Malware attacks like these are on the rise and continue to plague the mobile market.

Riskware

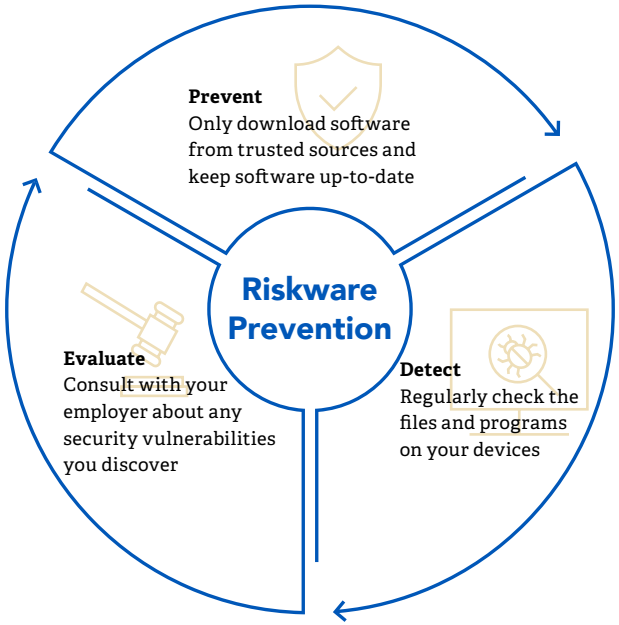
What is Riskware?

Riskware are legitimate programs that can cause damage if exploited by malicious users. Due to negligent security measures, riskware can poses risks to your personal data and to your device.

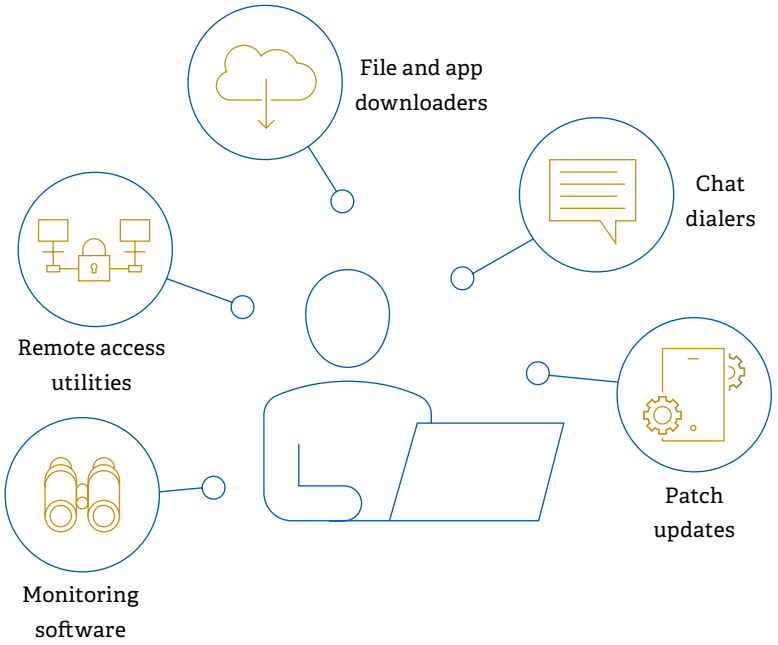
Riskware can:

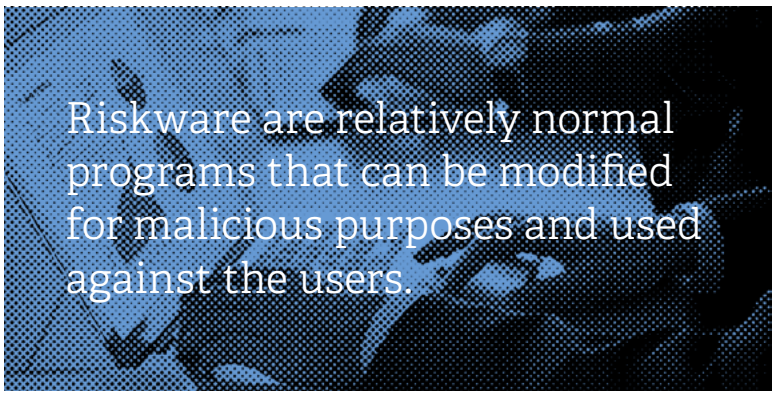
- ☐ Delete, block, modify or copy your data
- ☐ Disrupt the performance of your computers or networks

Applications aren't always intentionally malicious, but negligent security measures can pose a risk to your personal data and your devices. The login data or personal information you enter into an app is sent to a remote server; when that information is not secured or encrypted properly, it could be accessed by cybercriminals.

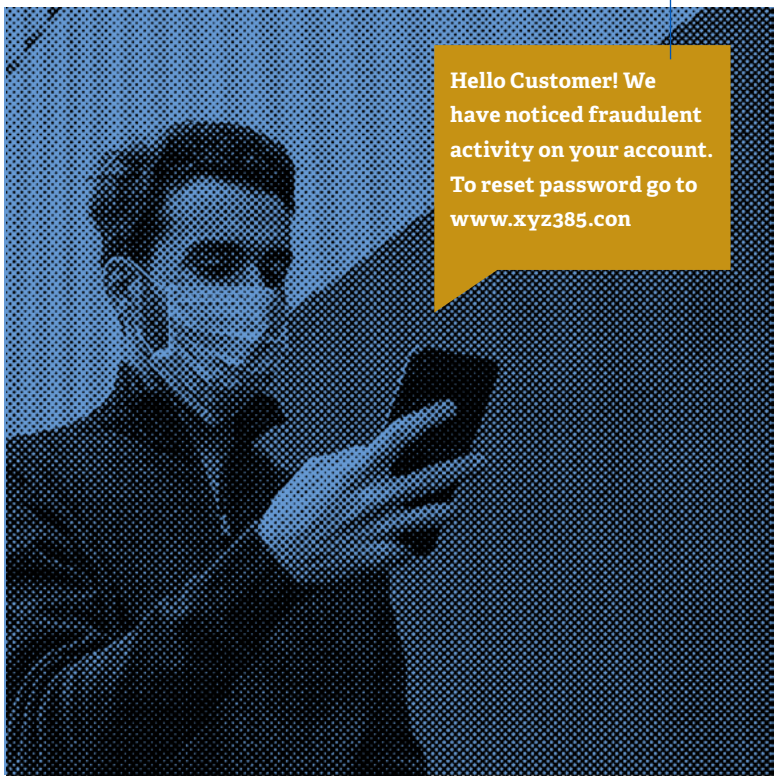


Types of Riskware





Mobile Device Signs of Infection



Performance issues or unusual activity may be a sign that your device has been compromised. When resources are stolen from the device for malicious purposes, there will be a noticeable difference in the performance of the device and you may receive notifications from your service provider about data overages.

Possible Signs of Infection

	Data Consumption: Unexplained data consumption or a higher phone bill occur
	Battery Drain: The device's battery drains more quickly than normal
	Crashing: Apps crash or the entire device malfunctions often
	Overheating: The device heats up quickly or chugs with no explanation
	False Notifications: False notifications and pop-ups start appearing on the device or within apps
	Unusual Communications: People claim you called them at odd hours or sent them strange text messages
	New Files: New apps or photos appear on your device that you did not install
	Unauthorized Purchases: You receive receipts or bills for unauthorized in-app purchases

Source:
globalworkplaceanalytics.com/work-at-home-after-covid-19-our-forecast

Examining Permissions

Before installing apps, examine the publisher, read the reviews and carefully look over the required permissions.

If it is a maps app, it is reasonable for it to access GPS location, but it seems unlikely that it would need to modify your device's storage.

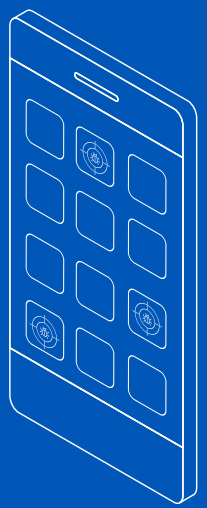
Be aware that some publishers have illegally paid for five star reviews to trick potential downloaders into believing that it is not a malicious application.

Consumers downloaded 204 billion mobile apps to their connected devices in 2019, up from 140 billion in 2016.

—Statista.com

Every day, 24,000 malicious apps are blocked - this high volume almost ensures that many are still getting through unidentified

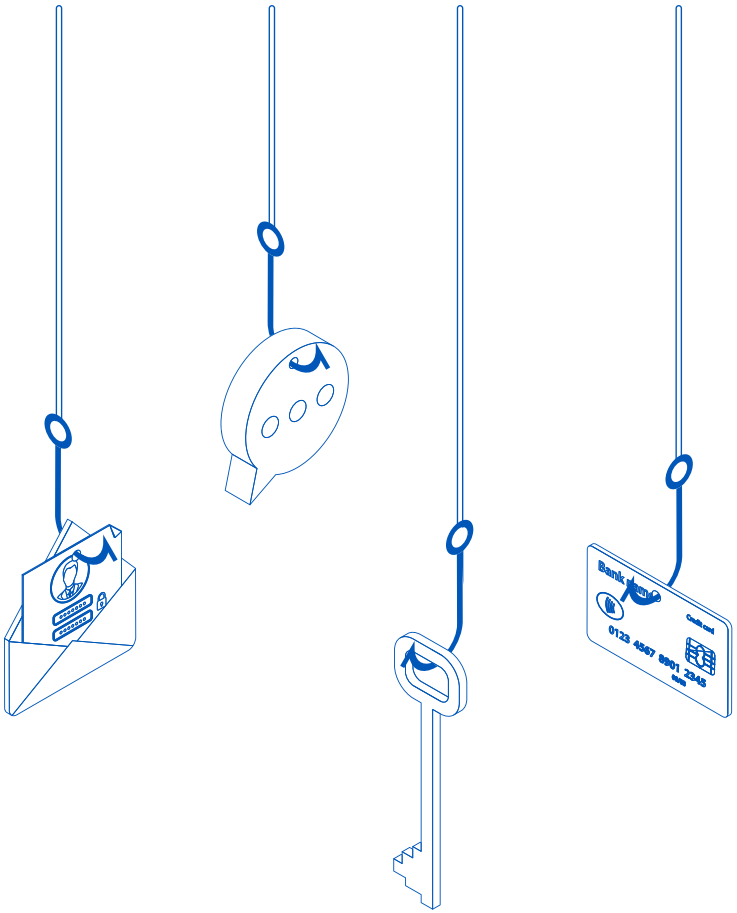
—Statista.com



Spear Phishing

Spear phishing is a type of phishing attack that targets a specific individual. Criminals will use information that they find online about their victims to trick them into believing that the communication is legitimate.

It can be difficult to spot a convincing spear phishing email. Avoid becoming a victim of spear phishing by examining the sender, not clicking unknown links or attachments, securing online profiles on social networks, using unique passwords across all of your accounts and updating your operating system and software when updates become available.



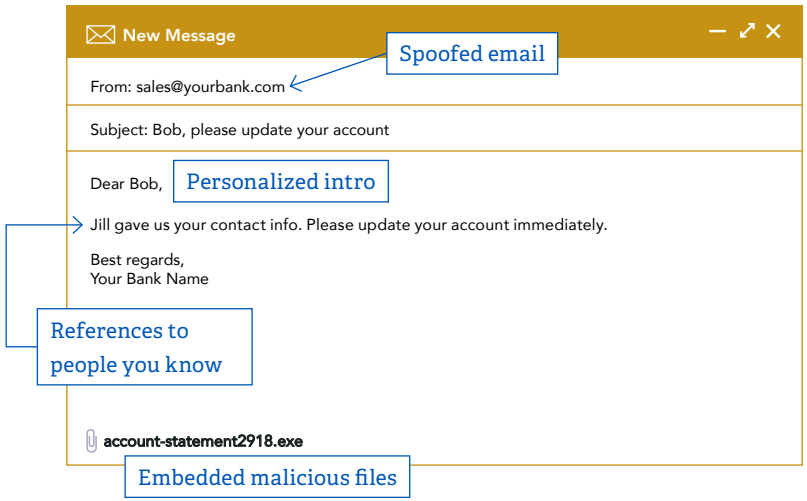
Identifying Spear Phishing

Spear phishing emails are a highly targeted attack method that will try to trick you by appearing legitimate. They may include personal information about you, refer to you by name, use familiar company logos or appear to come from a known contact.

To identify a possible spear phishing attempt:

- ☐ Check the sender and email address
- ☐ Be suspicious of emails containing links or attachments
- ☐ Don't immediately trust unusual emails that request sensitive information, ask you to click a link or download an attachment or request that immediate action be taken

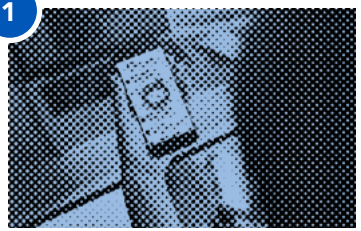
What to Look For



Spear Phishing Example

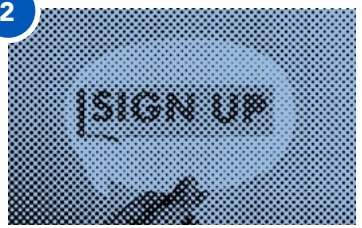
To fight spear phishing, you and your team should be aware of how to spot these emails. Traditional security methods often miss these attacks because they appear to be from trusted sources.

1



An email is sent to you claiming to represent a Software-as-a-Service (SaaS) provider. The email address appears to be legitimate.

2

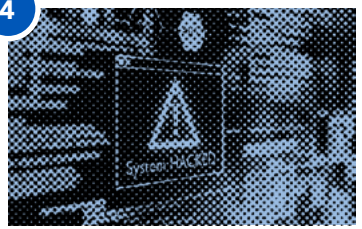


The email claims to offer a free new service for a limited time and invites you to sign up using the enclosed link.

3

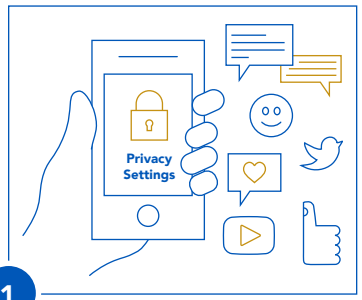
After clicking on the link, you are redirected to a login page on a fake website identical to the email.

4



An agent is installed on your machine, which can then be used as a backdoor into your enterprise's network.

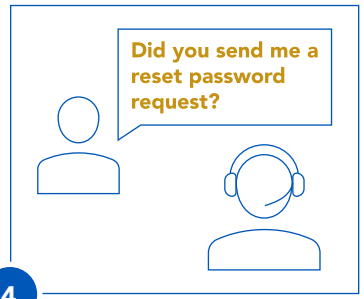
Spear Phishing Tactics



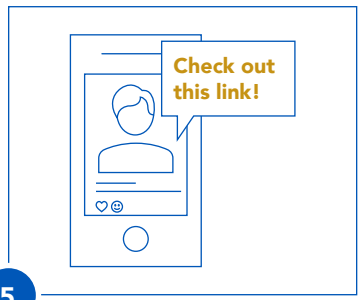
1 Attackers will research you online

2 Gaining your trust

3 Spoofed company emails



4 Hacking accounts

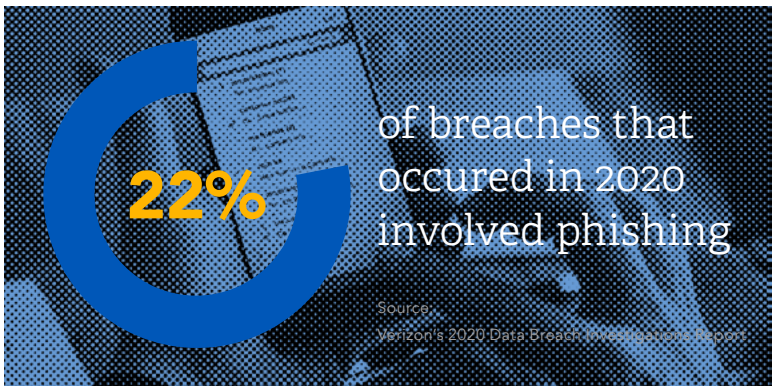


5 Spear phishing on social media

88% of organizations faced spear phishing in 2019

Source:
Proofpoint's 2020 State of Phish

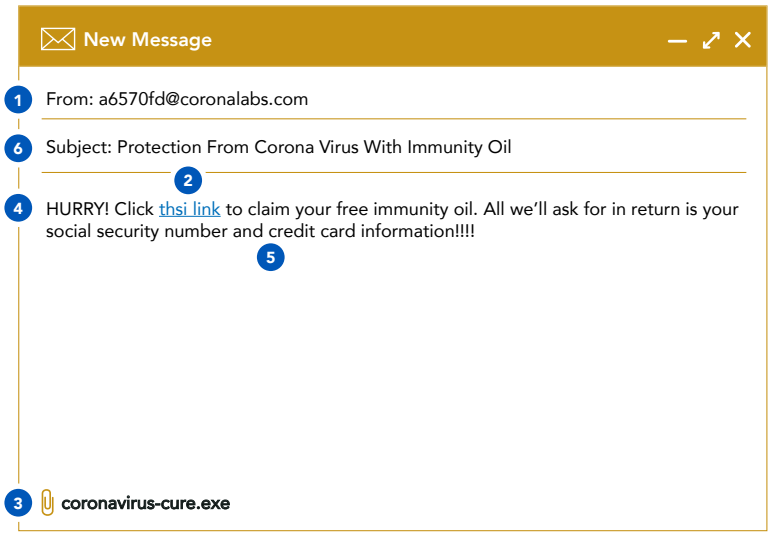
1. Be aware of your presence on social media and what personal information you share. Utilize privacy settings that are available on social media accounts and share only what is necessary.
2. Spear phishing criminals can target you via text message using similar tactics to make you click malicious links. The same tactics may be used on social network sites.
3. Spear phishing emails can appear legitimate by copying an authentic company email.
4. If you are sent a suspicious email, even from a trusted contact, err on the side of caution. Attempt other means of contact to confirm if the email is legitimate or if their account has been compromised.
5. Catphishing may be used to gain trust over a period of time. Be wary of communications with strangers and don't readily give out private information to contacts that you don't know.



COVID-19 Phishing Emails

As if we didn't have enough on our plates already, scammers and hackers are taking advantage of the global pandemic by targeting individuals with phishing emails – unsolicited emails posing as if sent from a trustworthy user or organization. They might be written in a way to elicit an emotional response from the receiver, persuading you to give out personal or corporate details. So what should you look out for?

Coronavirus-related domains are 50% more likely to be malicious than other domains



If it sounds too good to be true, **it probably is.**

1 False Senders

Often, scammers will create a spoof email address to make it look like the phishing scam has come from a legitimate source. Check out the sender's name and company suffix, if you know the person in real life, reach out to double check whether they sent the email.

2 Malicious Links

Coronavirus-themed or other crisis-related phishing emails may also contain some form of malicious link. Even if it looks safe enough, clicking a link could take you to a malicious site, download info-stealing software, install software with hidden malicious functionality (what we call a Trojan – hiding in plain sight), or even download ransomware onto your computer that takes your information and holds it to ransom. Not ideal.

3 Harmful Files

Similar to a malicious link, a phishing email might come with a file attached and instructions to download it. This could be a PDF, a Word document, or even an .exe file. Always be wary of downloading a file from an email. Scammers can be incredibly sophisticated and could replicate your office HR team with ease.

4 Immediate Action

Phishing emails, whether themed on the COVID-19 pandemic or not, will often call for some immediate action to be taken. Scammers tend to imply a sense of urgency in their emails to scare vulnerable receivers into making the download or clicking the link without fully considering the full outcome or possibility of a threat.

5 Requests for Details

Legitimate government agencies or banks will never ask you for your Social Security number, personal details or any sort of login information via an email. Anything asking for this, as well as banking information or passwords, could be a phishing scam.

04

Prevention

On the flip side of increasing threat activity, organizations have more incentive than ever before to identify, evaluate and mitigate threats. Protecting valuable data, adhering to stringent regulations, and maintaining healthy business operations have made threat prevention a higher priority. This section will examine best practices on how to minimize the risk of these prevalent threats.

Good Security Hygiene to Protect Against Malware

Malware can be avoided with good security hygiene. **Here are some tips to prevent malware infections on your devices:**

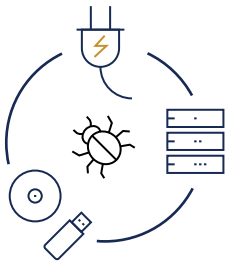
1

Use common sense and learn to identify the tactics most often used to deliver malware.

2

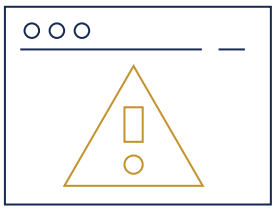
Regularly back up your files to prevent data loss.

3



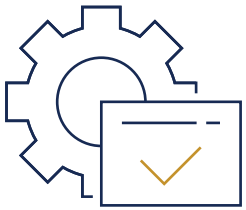
Be aware that external devices (USB thumb drives, USB hard drives, CD-ROM) or other seemingly benign USB chargers can be malicious and may contain malware that can infect your device.

4



Close unexpected pop-ups with your task manager software instead of clicking close within the pop-up to avoid sneaky malware installation triggers that cybercriminals hide in the close/exit button of a window.

5



Keep your software and operating system up to date to ensure that you're getting the latest security patches.

6

Use a secure firewall, run anti-virus software and scan your system regularly.

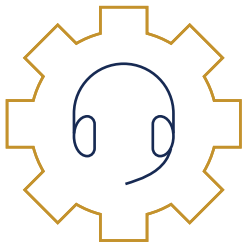
7

Use a secured WiFi network that has a strong password. Avoid connecting to public WiFi hotspots.

8

Be wary of browser plug-ins or mobile apps apps, especially those that were not published in the official app stores.

9

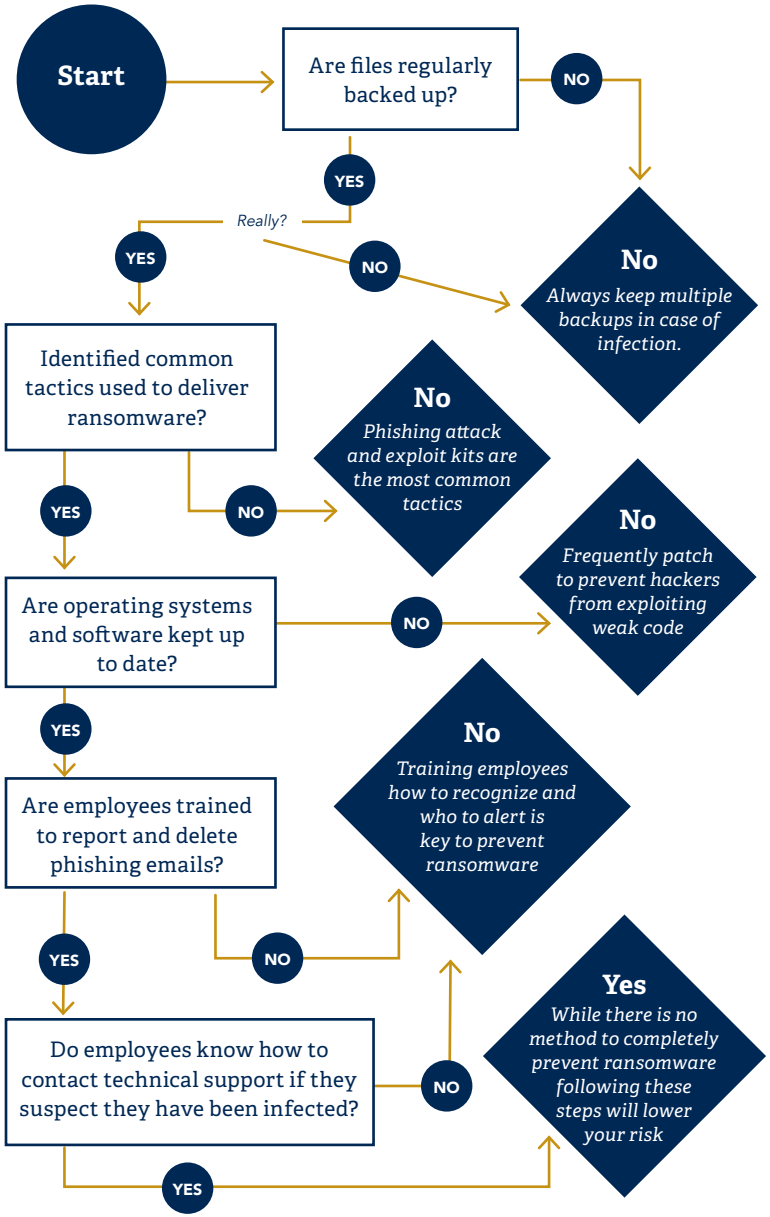


Contact technical support immediately if you suspect your device may be infected.

10

Report and delete phishing emails. Do not click unknown links or attachments.

Protecting Against Ransomware



Ransomware Trends

Ransomware targeting private users has been on the decline since the rise of cryptomining (the process by which new cryptocurrency is entered into circulation). According to experts, ransomware more commonly targets large organizations as opposed to individuals because it is more profitable for cybercriminals.

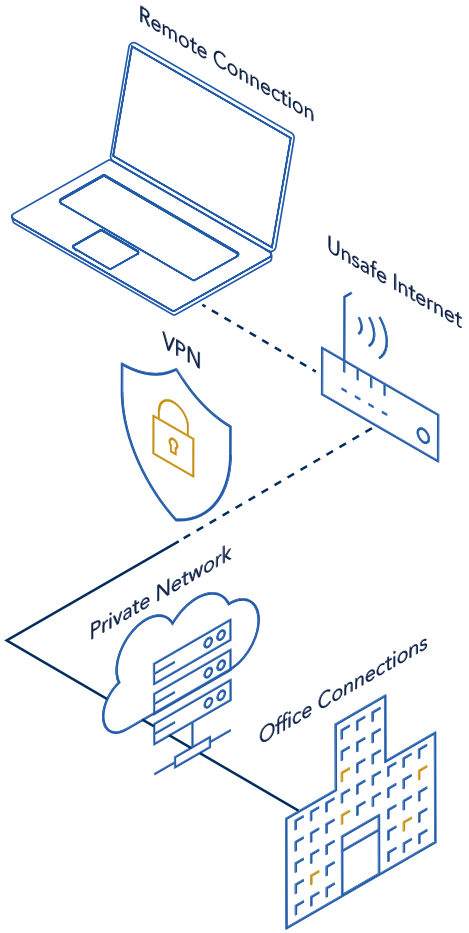
Mobile Device Security How-to

1. Keep your mobile devices' operating systems up-to-date
2. Avoid clicking unknown or suspicious links that may lead you to install malware
3. Turn on automatic app updates in your settings. Software updates patch known security vulnerabilities that can be leveraged to attack your device and access your personal data

How a VPN Works

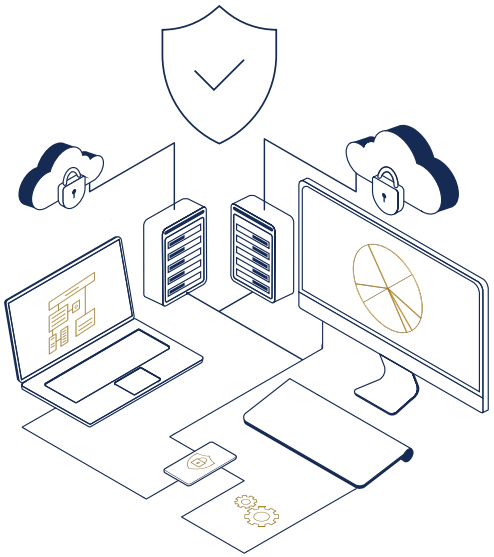
If your organization utilizes a virtual private network (VPN), once you are connected to the internet, use the VPN to connect to organizational systems and resources.

A VPN makes a **direct, secure connection between your device and the private network of your organization.** This connection is called a secure VPN tunnel.



VPN Checklist

The actionable technical steps outlined here provide the foundational support needed to enable and secure a work from home model.



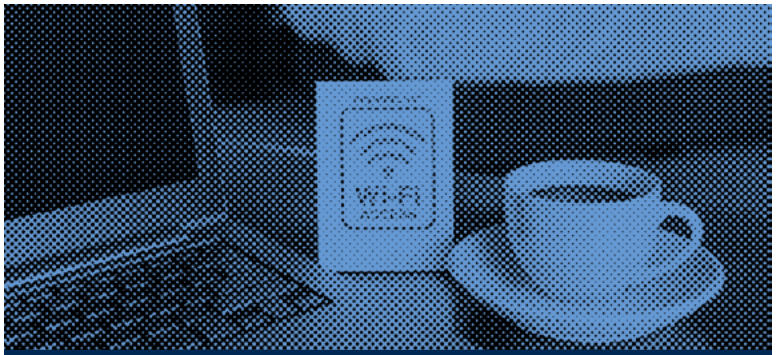
- [ ] Ensure certificates are installed properly and are properly chained; Ensure cryptography associated with installed certificates is strong; DO NOT use MD5 or SHA1 associated certificates
- [ ] Understand all aspects of your solution capacity (concurrent and/or total users), including users per appliance and technical specifications around capacity
- [ ] Know your solution's licensing model (concurrent vs. provisioned) and understand how to rapidly provision and de-provision licenses
- [ ] Discern all aspects of provisioning users and machines for remote access, ensuring user-facing documentation is up to date and accessible
- [ ] Measure current bandwidth and predict future bandwidth needs leveraging existing solution-monitoring tools

- [ ] Add additional internet circuits or upgrade to higher bandwidth circuits
- [ ] Meter VPN usage for both bandwidth and licensing concerns by introducing multiple shifts for workers to spread out the peak times for remote access usage
- [ ] Implement browser proxy through a VPN solution if the solution supports it for lower bandwidth internal applications
- [ ] Implement DNS security where possible to validate queries and block queries of malicious domains. A properly configured remote VPN solution will query in-tunnel DNS servers for internal resources
- [ ] Restrict non-essential traffic over VPN connections (e.g. limit non-essential URL categories)
- [ ] Configure full-tunneling VPN solutions if bandwidth is not an issue to reduce the attack surface area
- [ ] Allow split-tunneling for VPN connections in conjunction with a robust least-privilege policy for VPN traffic if bandwidth is a concern
- [ ] Validate your remote access endpoint enrollment process
- [ ] Review your update procedures and validation techniques for system patches and security solution updates using a remote access solution
- [ ] Use host checking capabilities to ensure compliance with policy – the asset type, the asset posture, etc. Use continuous host checking if the solution supports it
- [ ] Consider hardware VPN solutions (remote access points and others) for long-term WFH solutions

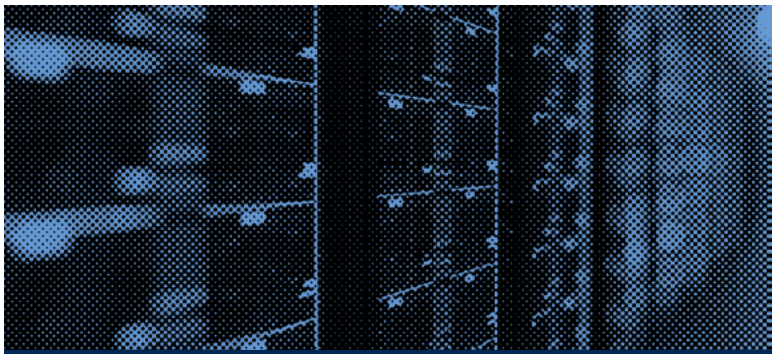
Source:
Optiv's COVID-19: Securing Work From Home Checklist

Vacant Facility Considerations

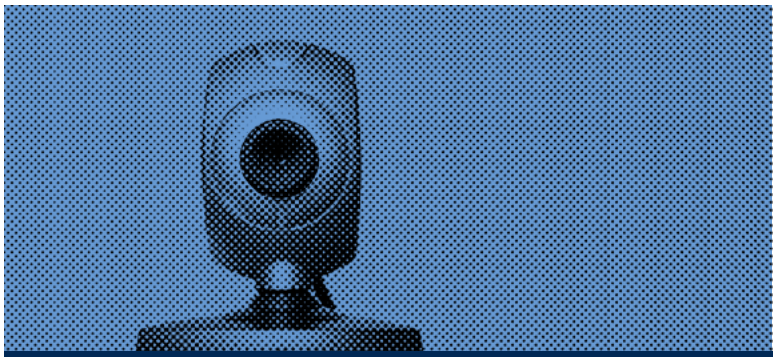
When crisis occurs, system administrators must often work from home, leaving facilities vacant and potentially exposing critical assets to cyber threats. Here are steps you can take to mitigate those risks.



Consider disabling guest WiFi and any other wireless access that is not well-secured as users will not be available to spot suspicious loitering around your facility.



Ensure that the temperatures are monitored, and alerts are sent remotely, especially for datacenter sites.



Look for ways to send audible failure alerts over your network (consider using web cams equipped with audio to provide visibility, if necessary).

Establish alternate receiving locations (i.e., shipper locations) for inbound deliveries to prevent potentially sensitive materials from being left in an unsecured location.

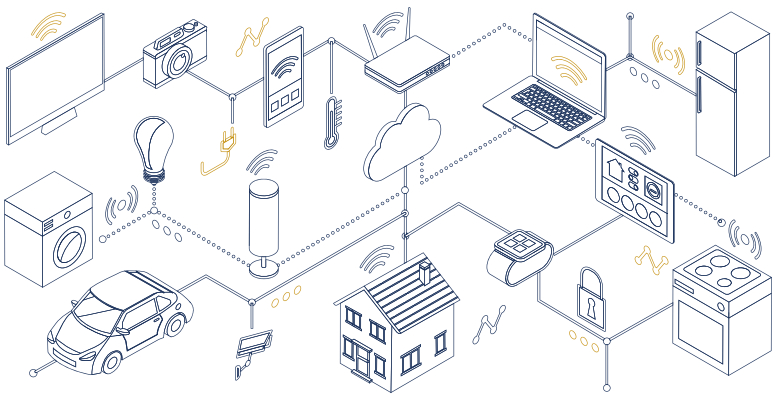
Make plans for any system that needs media physically rotated

Securing Work From Home

In times of crisis, enabling remote access for staff is the first priority for many organizations. Optiv has recommended three strategies for organizations to better enable more secure WFH environments: **expand existing access, create alternate access methods and redesign infrastructure.** Most organizations are performing some parts of each strategy to cope with the rapid expansion of remote workers.

While each of the organizations Optiv engages with are at differing levels of security program maturity, there are common themes in their program objectives. The good news is that the natural evolution of security enablement dovetails with providing expanded, easier-to-access services for employees and customers. Some of these common objectives are:

Ongoing objectives within the security organization are still valid and beneficial, even in times of rapid change. Continuing to execute on those core objectives helps bond existing cybersecurity principles to new projects and processes that arise when shifting towards a remote workforce.



Security Awareness Training
Regardless of the degree of cybersecurity controls that are put into place, humans still make bad decisions sometimes. Cybercriminals are using the daily media frenzy to their advantage. Organizations should continue to provide employees with routine cybersecurity training, reminders and tips.

Endpoint Security
Review mobile asset inventories and ensure that endpoint security agents are fully deployed and updated in order to combat the increased risk of malware. Additional considerations:

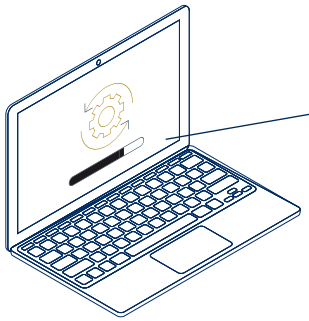
- Validate and publish the steps for remote endpoint security agent enrollment
- Implement host validation checks to ensure a minimum standard is met before allowing access to sensitive information
- Determine the level of access that will be permitted for bring your own device (BYOD)

Identity and Access Management
Regardless of the methods implemented to expand remote access, proper management of user identities will be the linchpin to a successful and secure rollout. The table stakes are ensuring that your directory services are accurate and accessible to remote applications.

SecOps
The change in system access methods will shift service loads and expose new capacity constraints. Ensure SecOps management is included in business line decision planning on remote workforce enablement. The operations team will need to stay abreast of dynamic changes in traffic flows, peak operating times and new sources of telemetry to incorporate with monitoring tools.

Securing Work From Home: Zoom Settings

1. Keep Zoom up-to-date

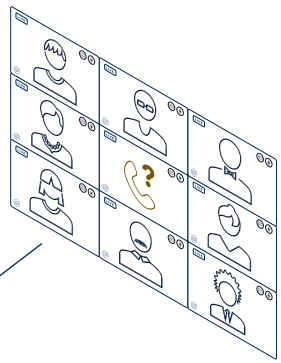


It's important to have the latest version of Zoom since they continuously release new and improved application security features

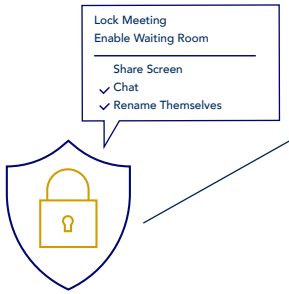
2. Prevent Zoom-bombing

Avoid hosting public meetings:

- Password protect your Zoom meetings
- Don't use your Personal Meeting ID
- Turn off 'Join Before Host' in your meeting settings so that you can monitor who joins the meeting. If you don't recognize an attendee, do not start the meeting until you've confirmed they should be there



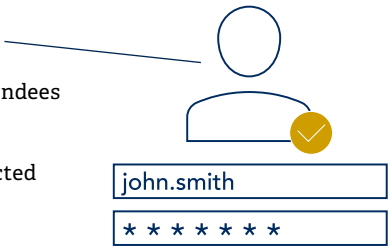
3. Manage security settings



Zoom's interface now has a Security icon that can be easily located in the host's meeting bar; these security settings were previously accessible through various menu settings

4. Manage your participants

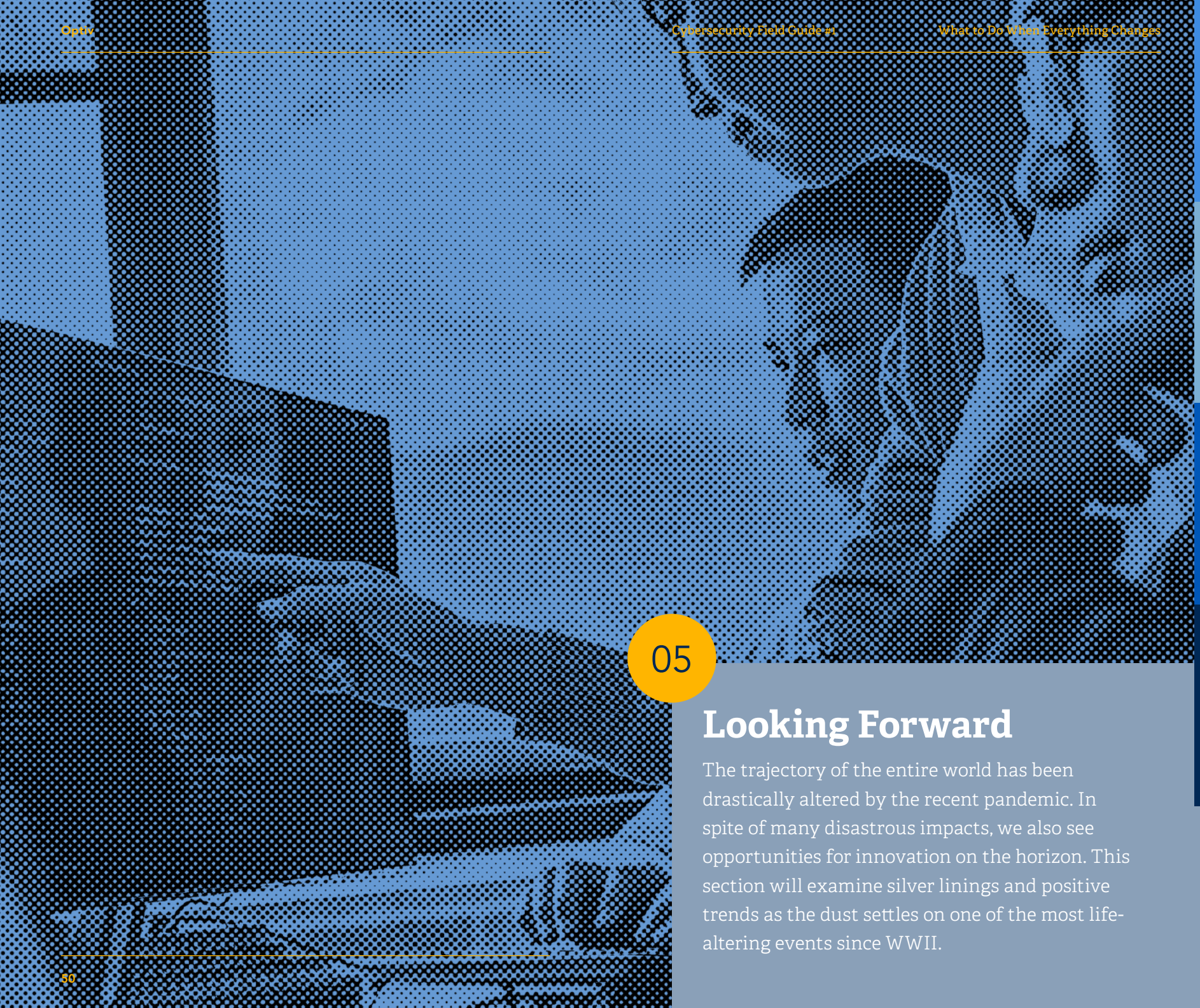
- Only allow signed-in user to join meetings
- Lock the meeting after all attendees are present
- Always use a password-protected meeting
- Disable private chat
- Turn on waiting room



5. Secure Zoom recordings

- Use local recordings by default
- If using cloud recordings, secure them through password protection and only enable authenticated users to view the individual recordings

Source:
"Settings for Securing Zoom", UC Berkley, https://security.berkeley.edu/resources/cybersecurity-and-covid-19/settings-securing-zoom



05

Looking Forward

The trajectory of the entire world has been drastically altered by the recent pandemic. In spite of many disastrous impacts, we also see opportunities for innovation on the horizon. This section will examine silver linings and positive trends as the dust settles on one of the most life-altering events since WWII.

Saved Costs of Working From Home

Many organizations were already embracing remote work to increase their ability to attract, retain and engage employees as well as reduce overhead costs and enhance sustainability. The COVID-19 pandemic prompted many organizations to launch or formalize these initiatives that may not have existed otherwise.[1]

Money Savings

On average, U.S. employers spend $86,000 a year ($400/day) in wages and benefits for every employee. If employees can't go into the office, it would pose a daily cost of $400/employee to the organization. However, having a proper remote working setup can mitigate these productivity losses.[1]

Space Savings

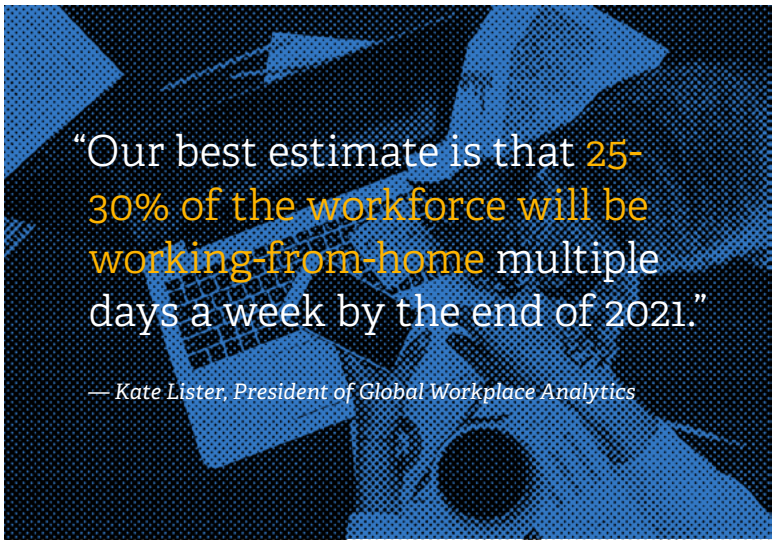
Less than 6% of our cities' roads have kept pace with demand; new roads are being built today to meet the needs identified up to ten or twenty year ago. At the current pace, we'll need an additional 104,000 lane miles to meet 2025 demands, which will cost $530+ billion. However, increased telework options would allow companies to invest in smaller office spaces while reducing the space impact from commuters.[3]

"If those federal workers who both can and want to work remotely did so just half of the time, the government could save up to $4B a year."[2]

Time Savings

Analysis from Best Buy, British Telecom, Dow Chemical and others show that **teleworkers are 35-40% more productive than their in-office counterparts.** In fact, Sun Microsystems found that employees spend 60% of the time they'd normally dedicate to commuting performing work for the company instead.

Remote working options can also enable employers to avoid brain-drain by retaining talent longer. 75% of retirees indicated that they'd be willing to continue working if they had the flexibility to still enjoy other aspects of retirement.[3]



Sources

1 globalworkplaceanalytics.com/brags/news-releases; Released in San Diego on May 4th, 2020
2 Kate Lister, President of Global Workplace Analytics
3 globalworkplaceanalytics.com/resources/costs-benefits; Advantages of Agile Work Strategies For Companies

Notes

Notes

Related Assets

White Paper
COVID-19: Overcoming an Abundance of Cybersecurity Caution →

Blog
COVID-19: From the Mindset of the Attacker →

Technical Checklist
COVID-19: Thwarting Opportunistic Attackers →

Blog
Securing Your Security Operations →

Technical Checklist
COVID-19: Hardening Security Operations →

Blog
How to Reduce Your Attack Surface →

Checklist
COVID-19: Securing Work From Home →

Want to learn more?

Visit www.optiv.com/contact-us

Secure your security.™

Optiv is a security solutions integrator – a "one-stop" trusted partner with a singular focus on cybersecurity. Our end-to-end cybersecurity capabilities span risk management and transformation, cyber digital transformation, threat management, cyber operations, identity and data management, and integration and innovation, helping organizations realize stronger, simpler and more cost-efficient cybersecurity programs that support business requirements and outcomes. At Optiv, we are leading a completely new approach to cybersecurity that enables clients to innovate their consumption models, integrate infrastructure and technology to maximize value, achieve measurable outcomes, and realize complete solutions and business alignment. For more information about Optiv, please visit us at www.optiv.com.

OPTIV

Optiv Global Headquarters
1144 15th Street, Suite 2900
Denver, CO 80202

800.574.0896 | optiv.com

11.20 | JH | 1.2