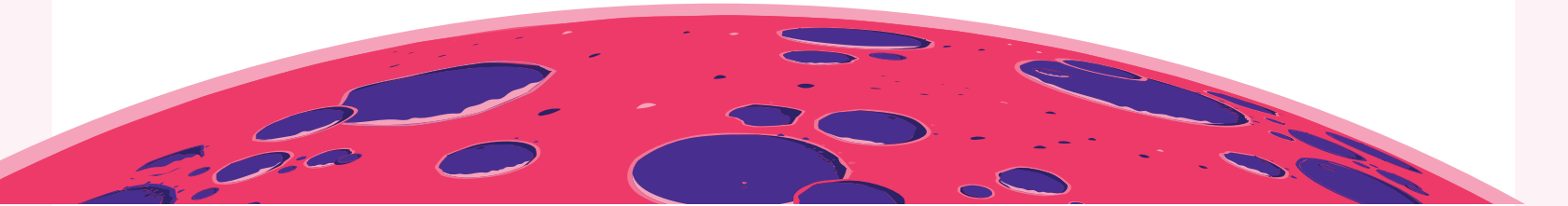
Infopercept
Secure . Optimize . Strengthen

A mysterious situation arises in today's Digital World as a result of Covid-19 Epidemic.

Report Date: **28-March-2020**

Infopercept
Secure . Optimize . Strengthen

Table of Content



Level 1

Malicious Campaigns

As the number of those suffering continue to surge by thousands,

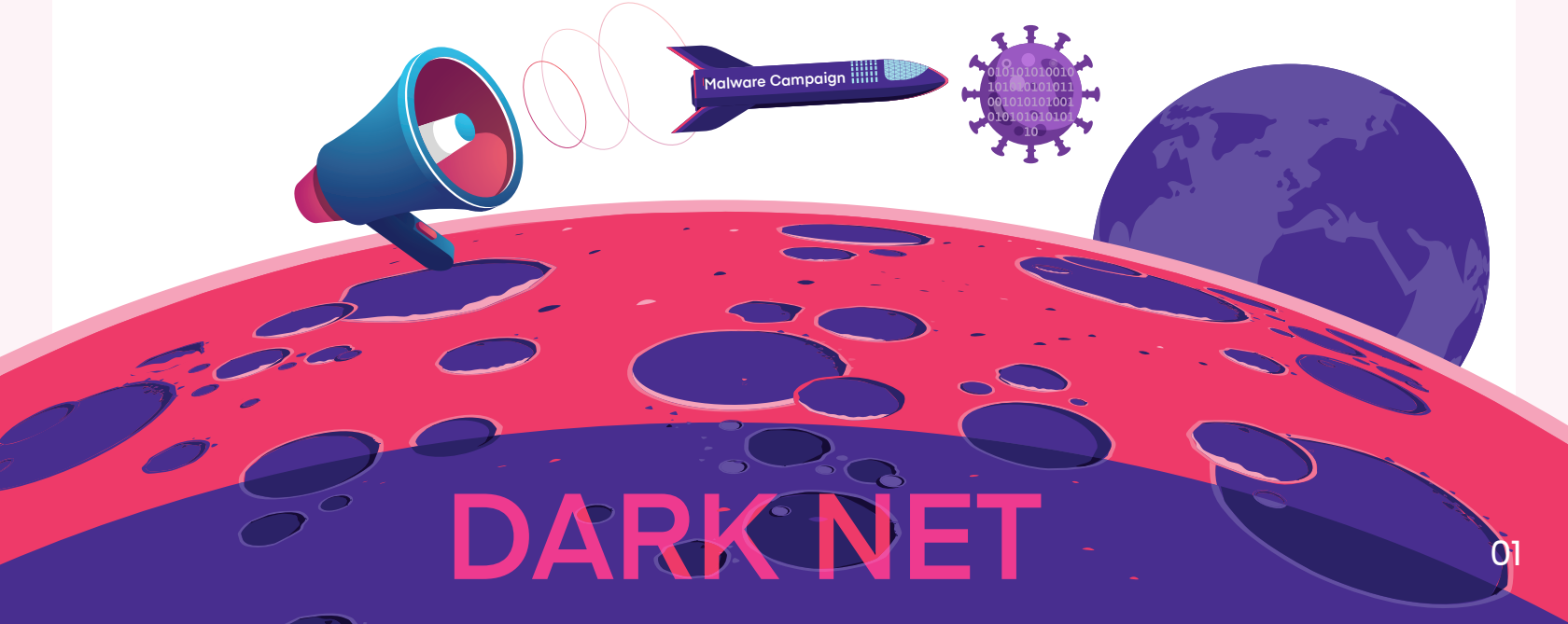
campaigns that use the disease as a lure are increasing likewise. Security Companies are continually researching and sourcing for samples on coronavirus related malicious campaigns. This report also includes detections from other researchers across the globe.

The novel corona virus disease (COVID-19) is being used in a variation of malicious campaigns

41% of companies affected

Malicious Key activities:

Email spam
Business Email Compromise
Malware
Ransomware
Malicious domains

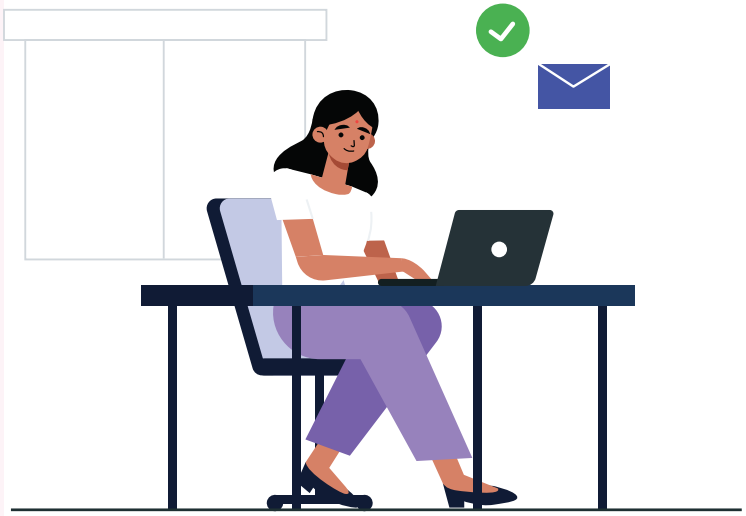


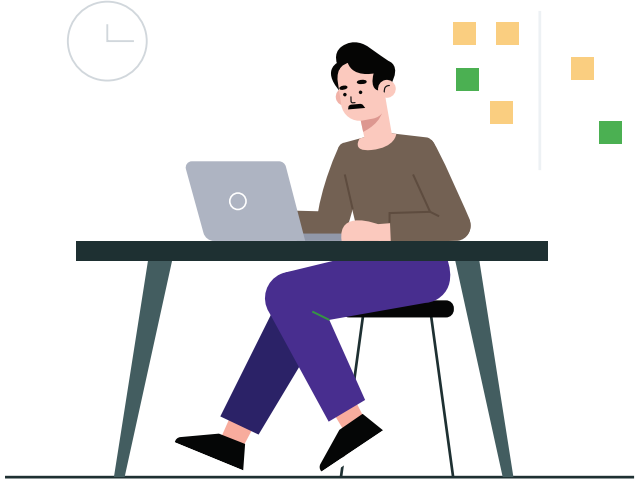
Level 2

Unknown, unknown Situation

Intellectuals foresee Coronavirus as the largest ever cyber security threat for Businesses

Consumers and businesses alike have been climbing to take steps to protect themselves from the coronavirus, from flocking to stores to buy out supplies of hand sanitizer, to encouraging workers to avoid large gatherings and work remotely.



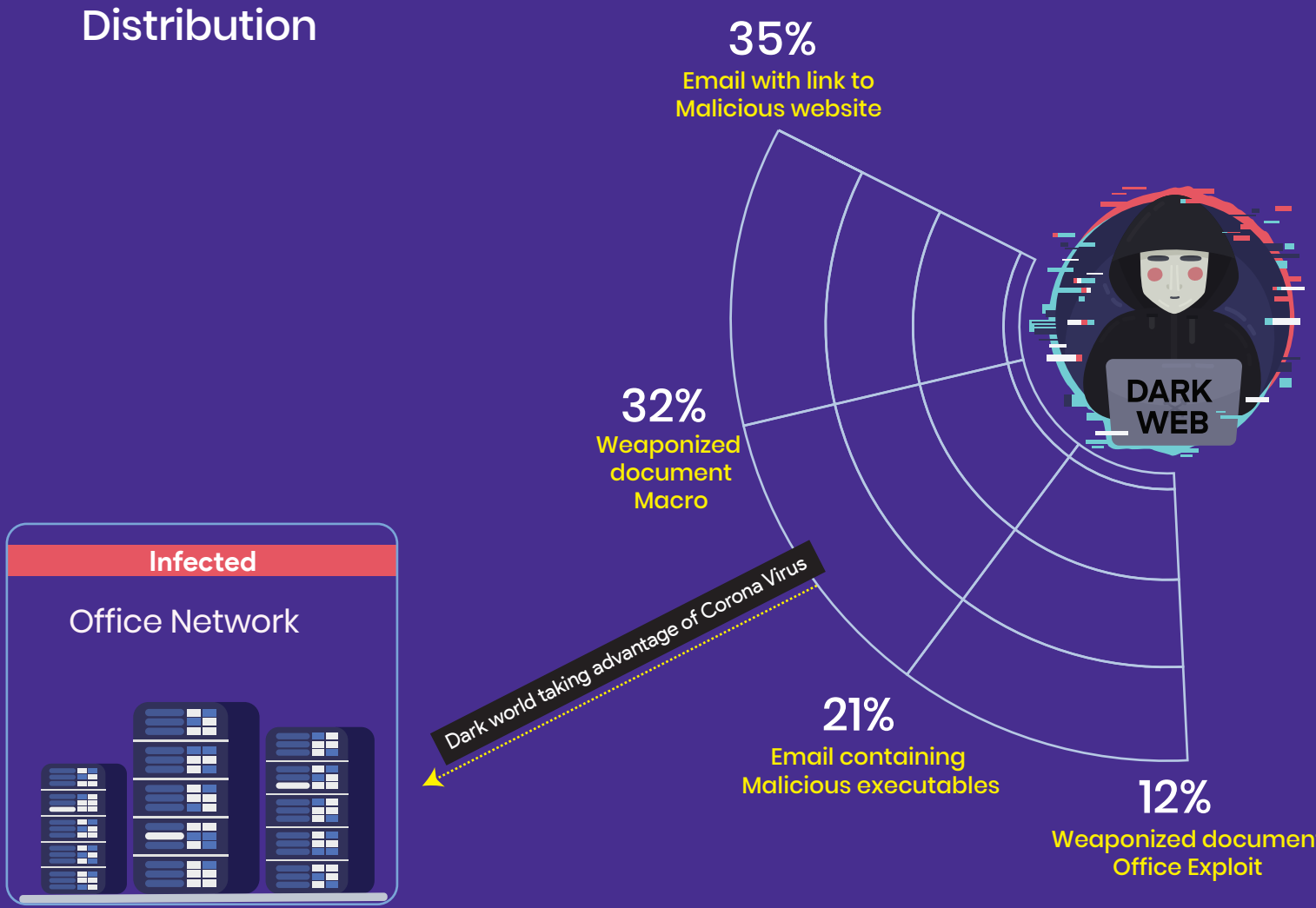


Level 2.1

The situation is forcing companies to adopt unchartered strategies to ensure Business Continuity with minimal or less focus on Cyber security as an aspect.

Dark-world is taking advantage of the situation to ensure more profits for themselves in these trying times.

Attack Vector Distribution

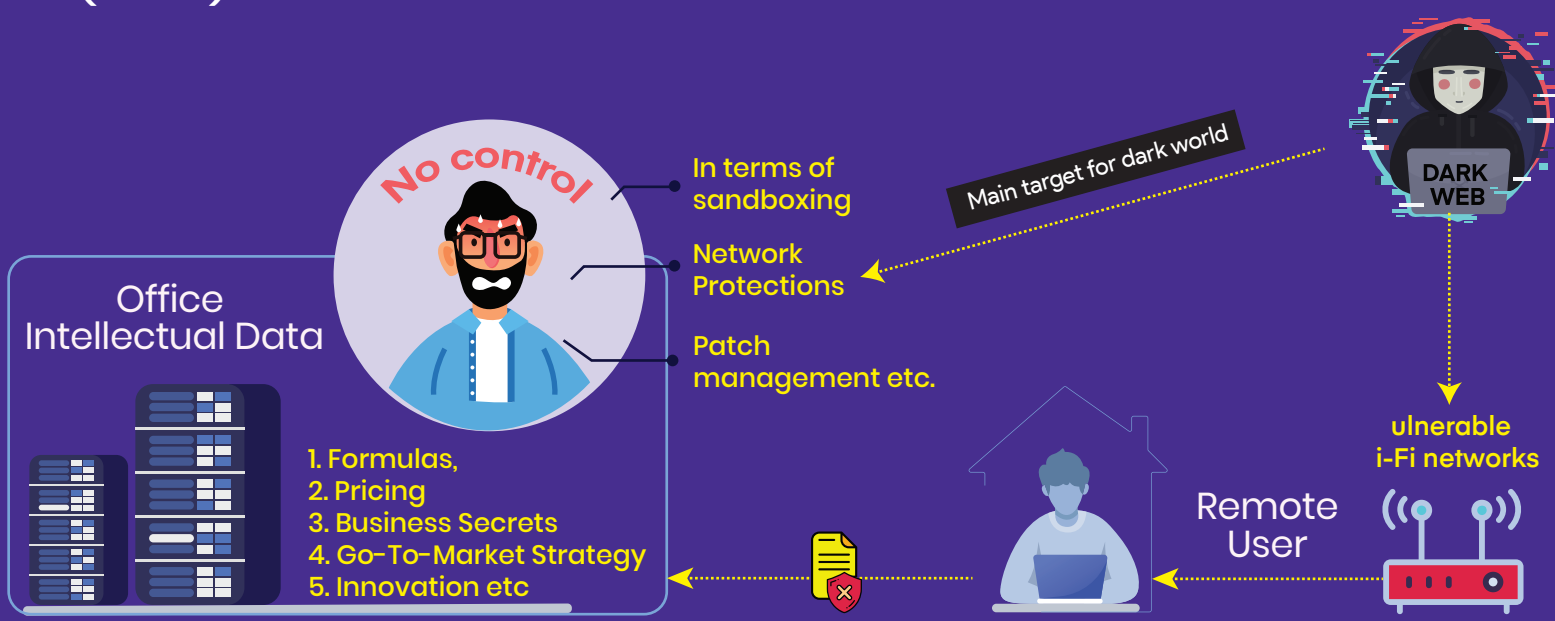


Level 3

What's in the minds of CEO's that is creating pressure on CIO's / CISO's / IT

The current need which is work remotely and completely distributed which is unknown unknown and where we business do not have much control (In terms of sandboxing, network protections, patch management etc.) on the end points which are always the main target for crooks / dark world.

CEO's are worried about the Intellectual property (Data) which could be in form of



Level 4

Concerns in this volatile environment for IT

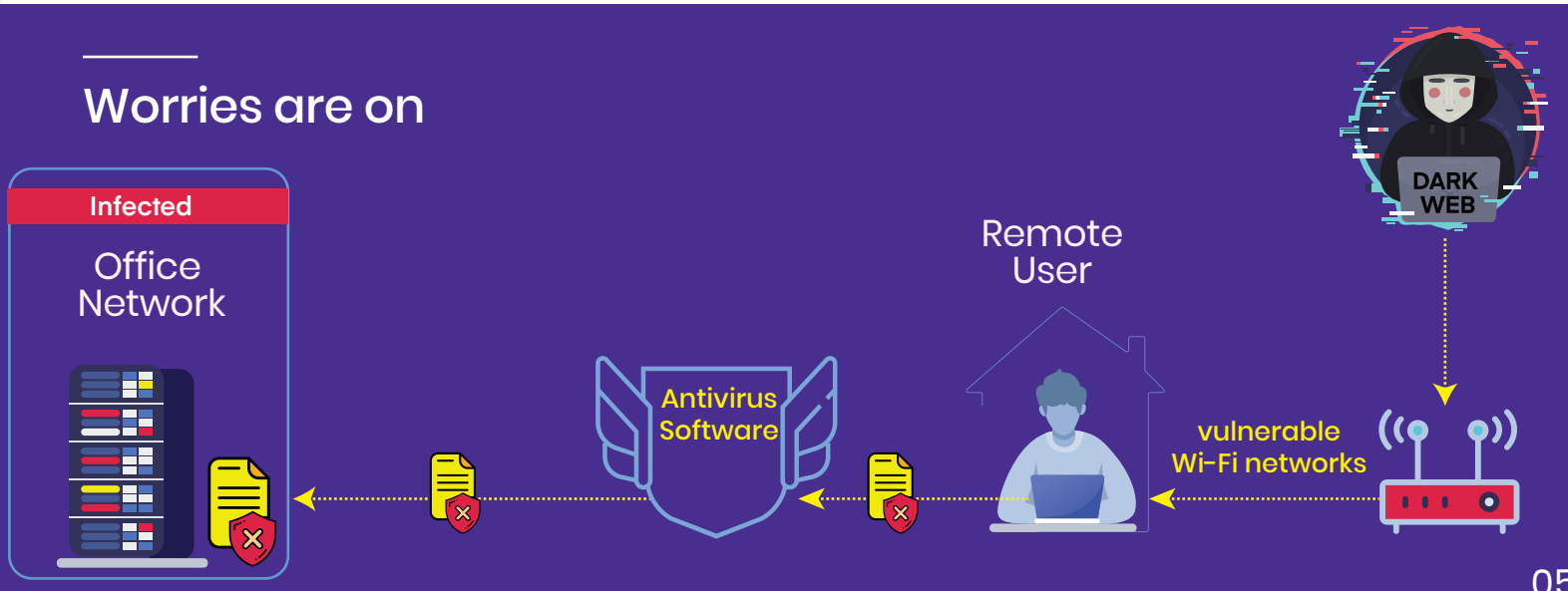
Is not with compliance, nor best practice nor secure remote user access with MFA nor Anti-Virus?

The CIOs and CISOs worries are on :

01. Biggest worry is dark web is targeting all the remote users and chances of executing advance attacks is the highest fear.

02. Worry of Threats which evades existing security solutions and creating point of persistence.

03. Is when this system (which is infected) will connect back with companies network, very high probability to affect horizontally. This will be a nightmare situation for any organization.



Level 4.1

Examples of Corona Themed Attacks

01. Fake websites to spread malware. Corona virus tracking app to target mobile devices.

02. Bypassing AVs using document sharing and advance attacks.

03. Trojan, Backdoor and advance phishing attacks using COVID-19 guideline document.

04. Remote user's endpoints connecting to vulnerable Wi-Fi networks where compromised systems are already part of network and it is horizontally infecting endpoints to get compromised.

05. CISA zeroed in on potential cyber attacks on virtual private networks (VPNs), which enable employees to access an organization's files remotely.

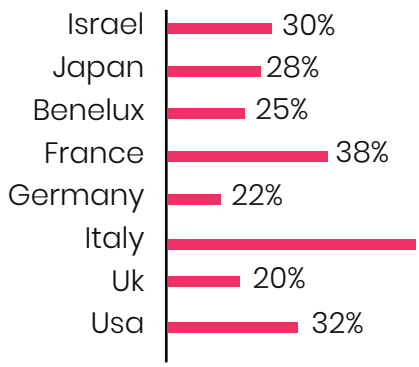
Corona Themed Attacks

Level 5

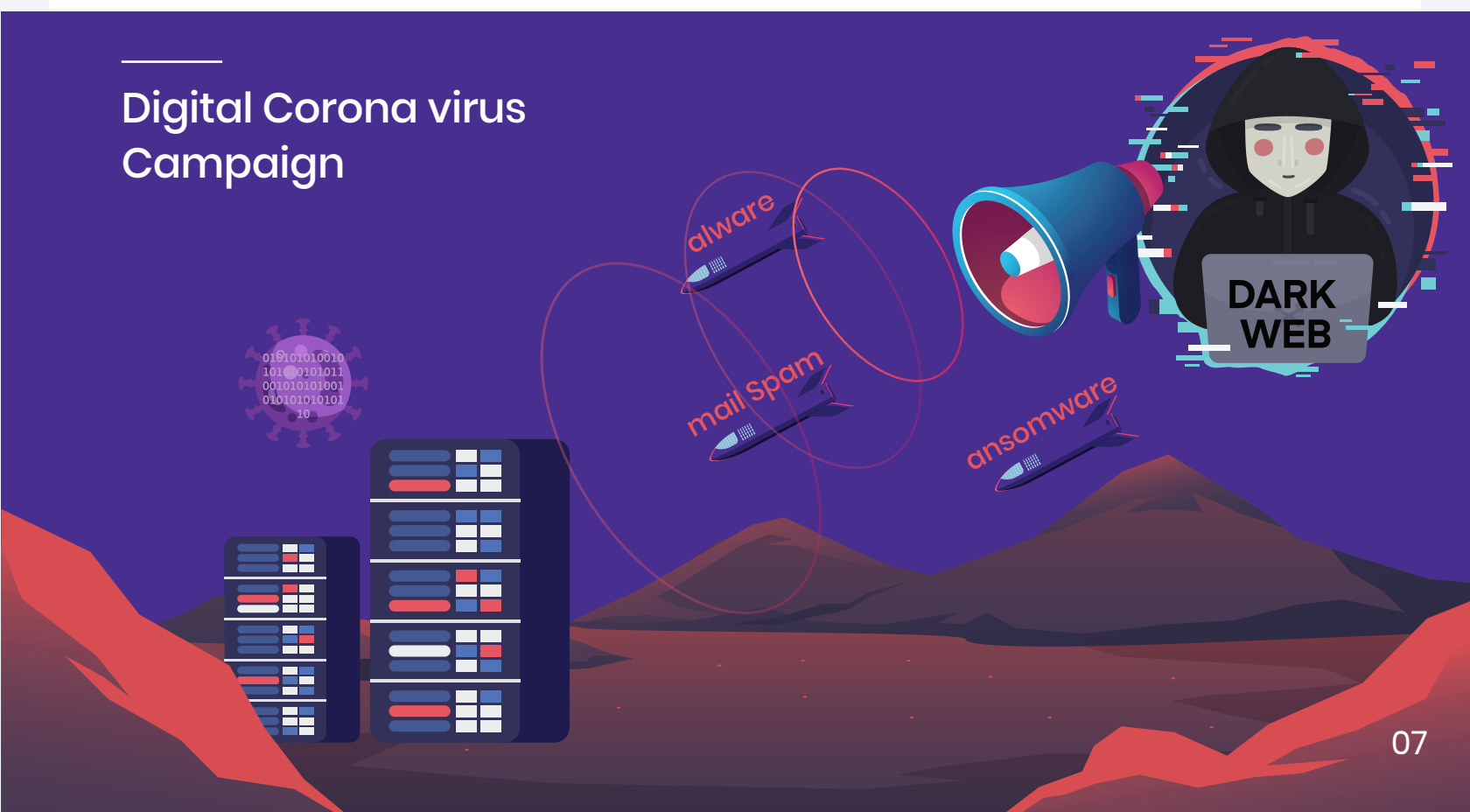
Coronavirus Used in Malicious Campaigns

The coronavirus disease (COVID-19) is being used in a variation of malicious campaigns counting email spam, Business Email Compromise, malware, ransomware, and malicious domains. Security Companies are continually researching and sourcing for samples on coronavirus-related malicious campaigns. This report also includes detections from other researchers across the globe.

Spike of Phishing Attacks in Italy



Digital Corona virus Campaign



Infopercept
Secure . Optimize . Strengthen

Level 6

Cyber Hygiene Measures for the Workforce and Consumers

We recognize the imminent threat posed by Corona- virus to not only the health of the general public but on business operations as well. Therefore, it is critical that business leaders take any necessary steps to ensure that business operations continue as close to the norm as possible.

While we hope our customers are taking the necessary steps to stay healthy (check out best practices from the World Health Organisation here, in addition to health risks, there are increased cybersecurity risks, too. The European Central Bank recently issued a warning to banks about the heightened potential for cybercrime and fraud, as many users are opting to stay at home and use remote banking services during the corona-virus outbreak. At a time of uncertainty and vulnerability for many, hackers and fraudsters are taking advantage of fear surrounding the virus as it continues to spread across the globe.

Warning to Bank about Cyber Fraud

Level 6.1

Follow Cyber Hygiene Steps

01. Avoid clicking on links in unsolicited emails and be wary of email attachments.

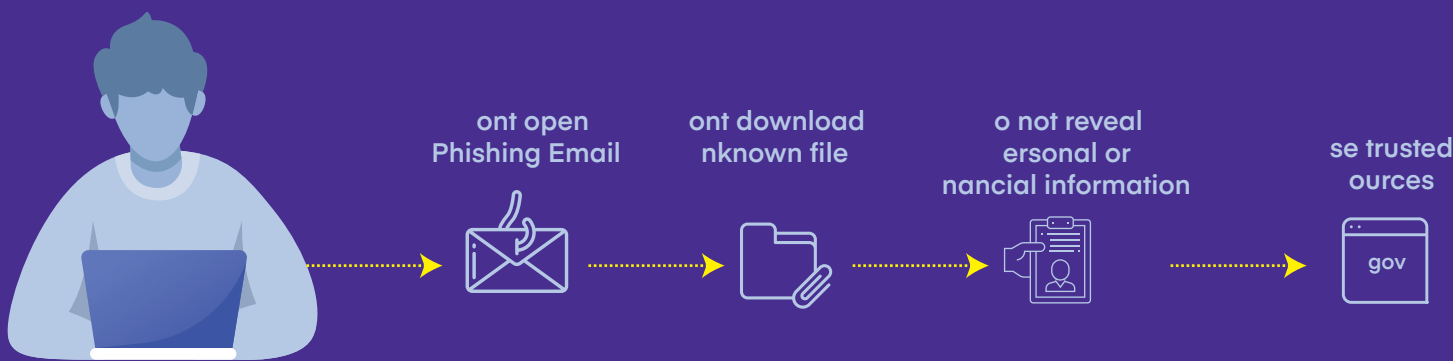
02. Do not reveal personal or financial information in emails, and do not respond to email solicitations for this information.

03. Review Tips on Avoiding Social Engineering and Phishing Scams for more information on recognizing and protecting against phishing.

04. Review the Federal Trade Commission's blog post on coronavirus scams for information on avoiding COVID-19 related scams.

05. Use trusted sources—such as legitimate, government websites—for up-to-date, fact-based information about COVID-19.

Follow Cyber Hygiene Steps



We'd love to talk to you about what this report means for your practice and your company.

Infopercept is committed to support 24*7 Top 7 Cybersecurity Hygiene Tips to improve the cybersecurity hygiene during this time

www.infopercept.com

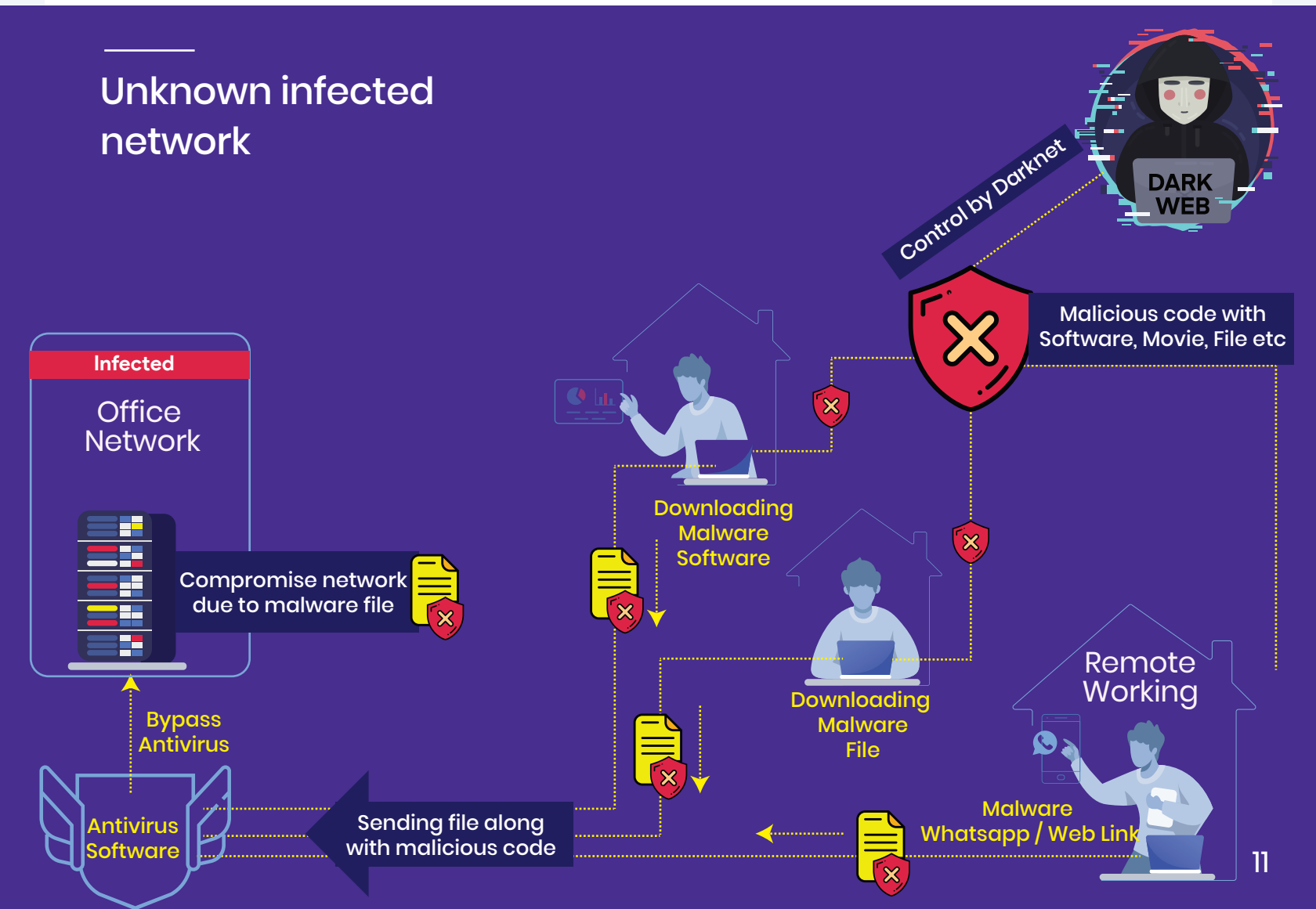
Infopercept
Secure . Optimize . Strengthen

Cybersecurity Hygiene Tip - 1

Implementing Strict control on end user systems in challenging times have practical limitations resulting in organizations relaxing control for end users. Risk of malware's infecting the systems bypassing the controls is very high and a challenging scenario since the existing solutions would have limitations against evasive attacks which are designed to bypass solutions. These attacks are classified as "FileLess" attacks.

<File less attacks at 51% follow link in WhatsApp> this will put a heavy load on the already stretched IT Security Operations team. Infopercept can address the risk by having a light weight agent deployed on endpoints to protect against unknown-unknown attacks and covering application virtual patching against memory evasive or file less attacks.

As agent does not require updates and has zero impact non-performance this will address the needs to business and security together in a way never envisaged formerly.



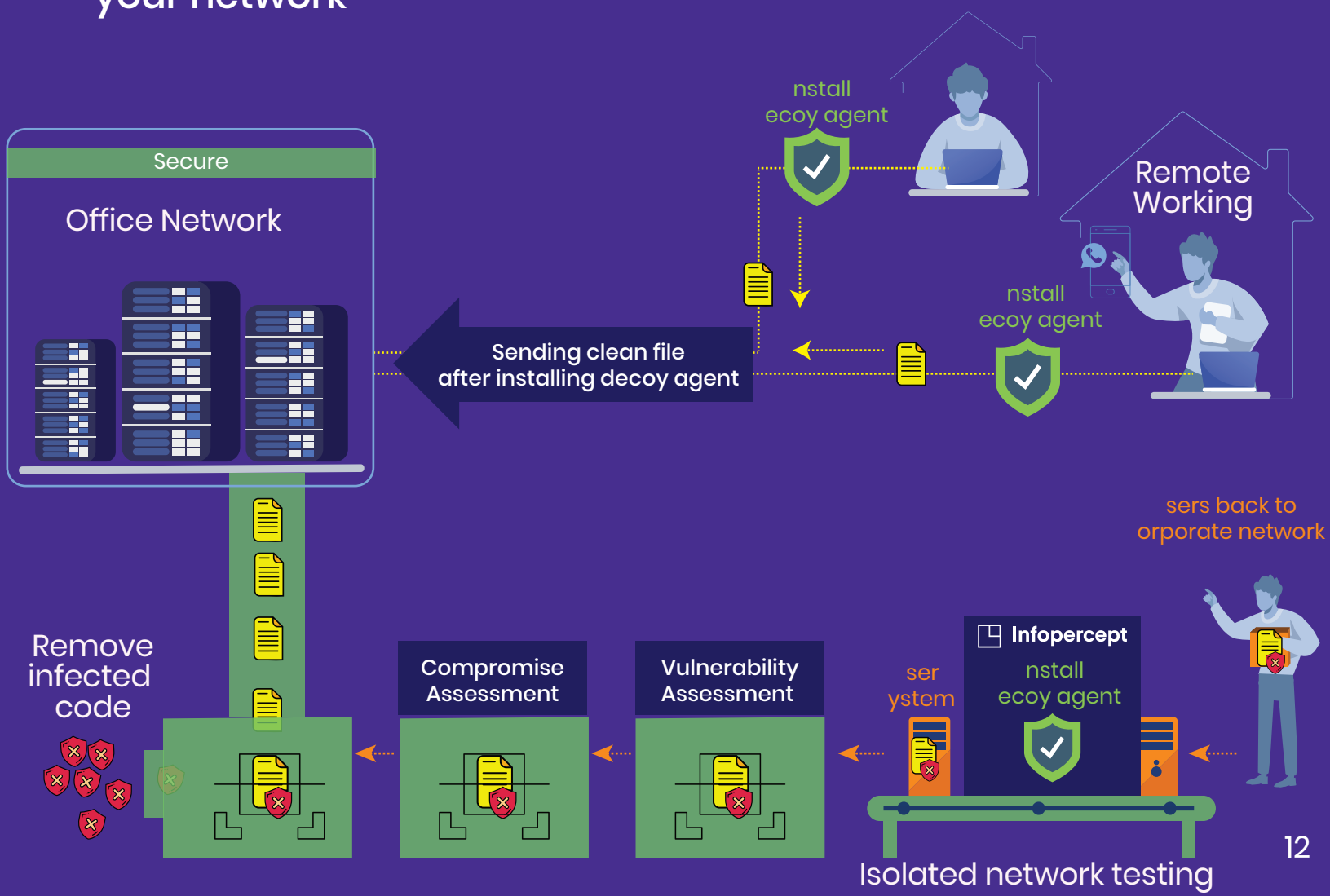
Cybersecurity Hygiene Tip - 2

Before allowing users back to corporate network perform compromise assessment, vulnerability assessment as this will be nightmare if the infected systems are able to spread horizontally in the network.

Infopercept will install decoys in the isolated network to conducted the testing / comprise assessment which is very similar to what the world did to tackle covid-19 quarantine foreign return people, perform testing and then allow them to return back home.

This will be very critical exercise for business globally.

How we secure your network



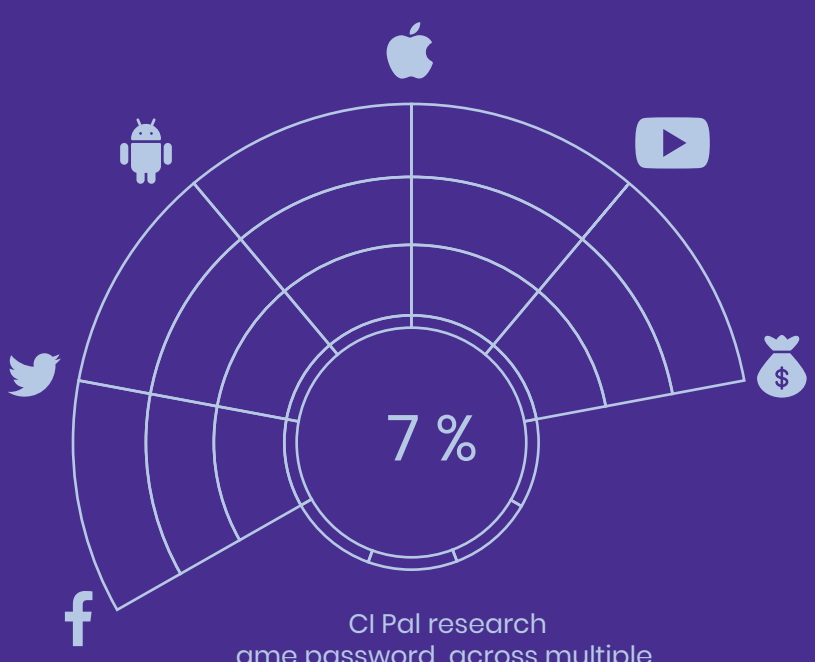
Cybersecurity Hygiene Tip - 3

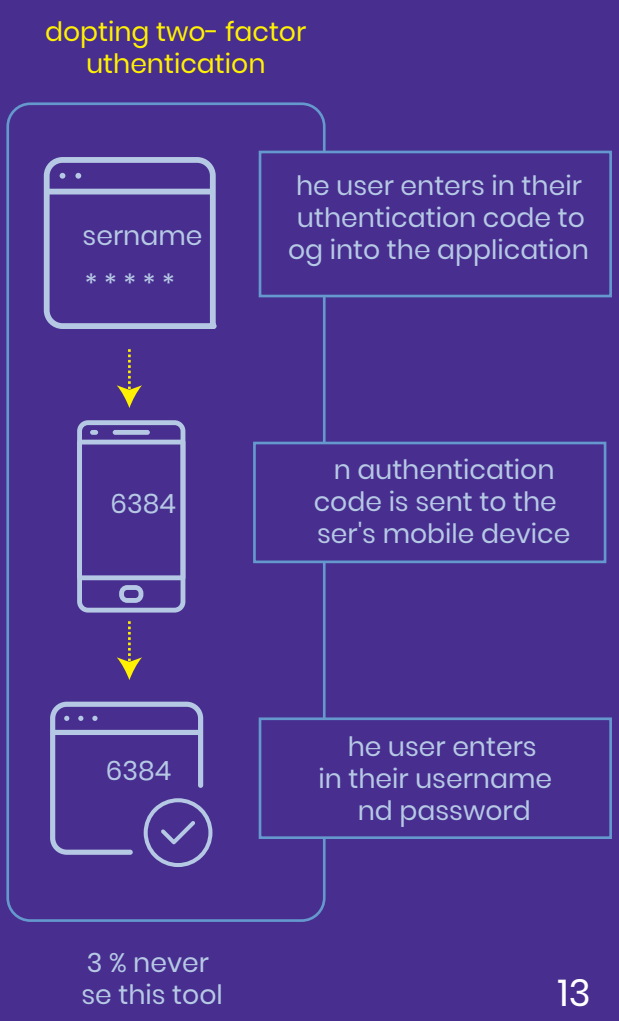
According to recent PCI Pal research, almost half (47%) of Americans use the same password across multiple sites and apps. We all know this is a big cybersecurity no-no, but it's especially important during times of heightened risk that we ensure our passwords are unique and secure. Consider updating your passwords and using a password manager tool to improve account security.

Cybersecurity Hygiene Tip - 4

In addition to varying passwords, consider adopting two-factor authentication for accounts – most services offer some sort of two-factor authentication, yet 23% of Americans report they have never used these tools to protect passwords or payments Take advantage of these tools – especially if you're going to be engaging with more digital services while you stay home to wait out coronavirus.

How to secure your account





Cybersecurity Hygiene Tip - 5

In addition to online fraud, there's also an increased risk for phone fraud – whether you're engaging with a customer service agent from your bank over the phone or simply ordering takeout. When speaking with a customer service representative, make sure you double check their credentials and only use the phone number provided by the company's website.

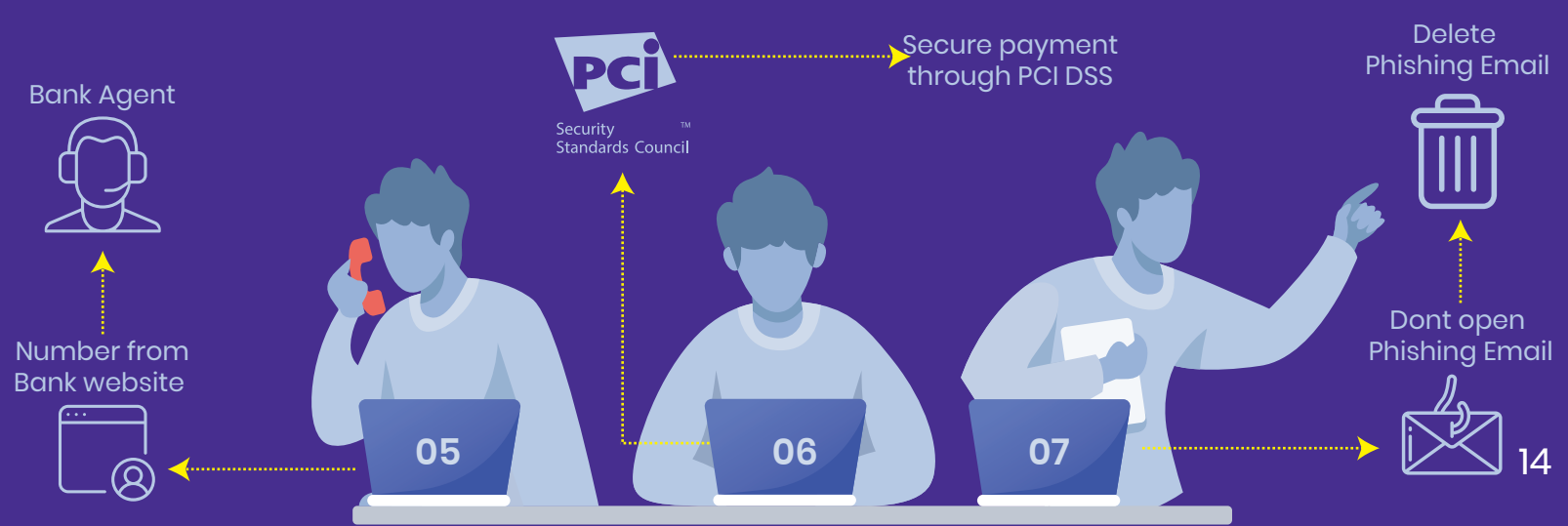
Cybersecurity Hygiene Tip - 6

For businesses looking to protect customer data during this time, consider PCI compliance, the strongest standard for payment security. PCI compliance standards can help protect your customers from data breaches and hacks – even when they ignore the above steps to protect themselves.

Cybersecurity Hygiene Tip - 7

Phishing scams relating to Coronavirus will be prevalent, including emails pretending to offer advice from governments and the World Health Organisation. Scammers will use such techniques to infect your laptop/PC and gain access into your systems. Every care should be taken before opening such communications.

How to Protect Yourself from Online Fraud



Infopercept
Secure . Optimize . Strengthen

We'd love to talk to you about what this report means for your practice and your company.

Email
sos@infopercept.com

Website
www.infopercept.com

Phone
+91 989 8857 117