CARBONITE® an opentext™ company | WEBROOT® an opentext™ company

HACKER PERSONAS

A Deeper Look Into Cybercrime

INTRODUCTION

Staying informed on today's ever-changing cybersecurity landscape is vital for mitigating threats and keeping businesses safe. This educational eBook, the sequel to the popular "Why Hacker's Hack" series, explores cybercriminal personas and who is most likely to fall prey to these scam artists. Learn why it's important to get informed on their methods, motives and strategies of choice. IT security experts Tyler Moffitt, Kelvin Murray, Grayson Milbourne, George Anderson and Jonathan Barnett offer advice to help you navigate today's evolving threats and the types of attacks to look out for. Continue reading to learn how to improve cyber resilience and help to keep your business online—no matter what surprises come your way!

What's Inside?

1 THE IMPERSONATOR

Today's cybercriminals are masters at exploiting basic human trust and impersonators have unfortunately perfected this technique. Pretending to be someone else, these hackers rely on vulnerabilities to manipulate their victims into opening doors to systems or unwittingly sharing sensitive data such as passwords or banking details. What makes this type of cybercriminal a massive threat is their expert ability to hide in plain sight, often masking their true intentions behind seemingly innocuous requests or legitimate-looking websites.

Who Falls Victim to Impersonators?

Many users are growing more educated about their attacks, but impersonators are increasingly sophisticated, often hosting malicious content on legitimate sites. Impersonators leverage trusted brand names, and those who let their guard down can easily fall prey. Phishing attempts can slip through DNS and endpoint protection, which makes security awareness training a must-have tool. Case in point, recent impersonation attacks prove consequences can be costly:

Twitter Bitcoin Scam
Over 130 high-profile Twitter accounts were hijacked and unsuspecting victims sent bitcoin to a fake cryptocurrency wallet with the promise of doubling the sender's investment. Over $110,000 USD was lost.[1]

Shark Tank Phishing Attack
A great example of how no one is immune, Shark Tank's Barbara Corcoran was a victim of a targeted phishing attack, which led to a payout of $388,700 USD for a false real estate renovation. The money was never recovered.[2]

Texas School District Scam
Manor Independent School District (MISD) in Texas fell victim to a phishing attack that cost them an estimated $2.3 million USD when an employee was tricked into altering bank account information for a vendor.[3]

> "The best way to protect your business is through a layered approach that incorporates both security software and security awareness training for every employee."
>
> **George Anderson,** Webroot

Phishing Attacks Continue to Haunt Businesses

Phishing, the preferred tried-and true method of impersonators, is one of the most common forms of cybercrime, and includes many different forms of attack, most prominently using fake email addresses and web domains. Phishing scams typically involve an impersonator masquerading as a higher-level executive to send emails that include malicious files ready to download or links to fraudulent web pages that request sensitive data, such as passwords, logins or credit card information.

BEC Attacks Are Gaining Momentum

The most common method of email phishing is known as business email compromise (BEC). These attacks are generally targeted at corporate employees, particularly in customer-facing roles. Impersonators slightly modify an email address and then send a request for a wire transfer or payment that doesn't stand out as unusual. For example, an event coordinator may regularly purchase gift cards for clients, so a request for a $50 gift card from the boss won't seem out of place.

Watch for Domain Spoofs & Malicious IPs

Businesses should be on the lookout for phishing attacks where impersonators trick victims by redirecting traffic to duplicate, legitimate-looking website IP addresses where they end up mistakenly entering sensitive data.

Phishing is so effective because it works. In a 2019 survey, 79% of respondents claimed they could distinguish phishing from genuine email, but nearly half admitted to clicking a link from unknown senders and 29% did so repeatedly.[4]

The Rise of Deep Fakes and AI-Driven Attacks

Deep fakes are a relatively new threat, but they have serious potential to wreak havoc. Criminals leverage media in which a person's image or voice is replaced with someone else's likeness with the intent to deceive. Although deep fakes have garnered attention for their use in fake news and celebrity hoaxes, business owners have cause for concern: one of the earliest examples of this attack vector involved the use of AI-based software to mimic the voice of a company CEO who demanded a wire transfer of $243,000 to a supplier.[5] The attack was ultimately successful.

HUMANS ARE THE WEAKEST LINK

Humans are typically the weakest link in the cybersecurity chain of defense, making social engineering a significant risk to organizations of all sizes.

Everyone, from receptionists to executives to IT personnel are potential victims of an impersonator. In fact, help desk and call center employees are especially vulnerable because they are trained to be forthcoming with information.

Effective impersonators can obtain valuable data such as user passwords, security badges, intellectual property, confidential financial reports, private employee information, and even other personally identifiable information like health records or credit card information.

2 THE OPPORTUNIST

Opportunists capitalize on unpreparedness, often exploiting common human traits such as trust and familiarity. They rely on targeted or focused attacks, and carry out their crimes against specific businesses or individuals. They are usually well planned, with hackers thoroughly researching their victims and running tests before performing an actual attack. What's more, opportunists look for existing weaknesses or vulnerabilities they can exploit en masse to pull as many victims as possible into their nets. In fact, by August 2020, the FBI saw a 300% increase in cybercrime related to attacks of opportunity.[6]

Opportunists Are a Threat to Everyone

Hackers use any opportunity to abuse victims by leveraging humanitarian crises and current events. For example, the global pandemic has led to a monumental rise in digital connectivity, creating a hotbed for cybercrime. These are just a few of their tricks of the trade:

Fake Covid-19 Trackers
Coronavirus trackers, which seem legitimate, can be hosts for malware and bots. In roughly the first half of 2020, more than 136,000 new domains were registered that reference COVID-19. A large portion of these sites distribute phishing campaigns that include pandemic buzzwords.[7]

Ryuk and Conti Ransomware
An increasingly common tactic for big ransomware groups is to create "leak sites" where they upload and leak sensitive documents from companies that refuse to pay a ransomware decryption fee. Cybercrime groups Conti and Ryuk are known for using leak sites to launch opportunistic attacks.[8]

Fake Charity Websites
No matter if it is a forest fire, hurricane or earthquake, cybercriminals are locked and loaded, and ready to take advantage of compassionate individuals. And many of these well-meaning victims never realize their donation failed to support their cause.[9]

> "The increase in remote work makes it easier than ever for cybercriminals to trick people into going to malicious websites because they're not protecting every endpoint and device."
>
> **Kelvin Murray,** Webroot

Work From Home Adds New Risks

The surge in remote work has heightened cyber risks for both individual employees and organizations. The biggest security challenges to telework include an increase in phishing attacks, enhanced risk of cyberattack on the company network, and potential disruption to business continuity. Because remote workers are not on the organization's network, the IT team can't be in control of every device. This essentially expands the attack surface, creating new vulnerabilities that hackers can exploit. As a result, IT teams have an increasingly difficult time ensuring uniform cybersecurity practices, leaving the business open to attack.

With so many people working from home, hackers are finding new ways to attack businesses. Video conferencing has become a critical tool for many users who need to connect virtually. Unfortunately, vulnerabilities in popular platforms can be open doors to cybercriminals. The FBI warned users about "Zoombombing," in which uninvited people hijack video meetings to cause disruption. In one such example, users hijacked a city meeting to harass users with slurs and profanities.[10] However, these attacks can also lead to more serious repercussions. Earlier in 2020, one video conferencing platform was found to be routing internet traffic through a foreign state, raising concerns about privacy.[11]

Of course, even with new threats emerging daily, remote workers are still vulnerable to the age-old tricks of the trade. Remote Desktop Protocol (RDP), for example, is still a major threat to every business. Cybercriminals can easily find and target organizations by scanning for open RPD connections on TCP ports and then brute-forcing the credentials. Even lesser-skilled criminals can simply buy RDP access to already-hacked machines on the dark web.

Opportunists Will Target Any Business

While some cybercriminals specialize in targeting large enterprises or governments, opportunists will target anyone – whenever the opportunity arises! This means every business is at risk of attack, and business leaders need to ensure that every employee is properly protected, both from a technology standpoint and through continued security awareness training.

THE RISE OF MISINFORMATION

Cybercriminals have not only taken advantage of the pandemic to make a profit through malware and phishing, they have used it to spread misinformation. In mid-March 2020, hackers used bogus text messages to spread false details of an impending national quarantine owing to COVID-19.[12]

What's more, in a one-month period, one country reported 290 fake online postings about the pandemic with the majority containing both false information and concealed malware. There are also reports of misinformation being linked to the illegal trade of fraudulent medical commodities.[13]

Even the World Health Organization (WHO) and the U.S. Health and Human Services Department (HHS) were targeted by nation-state phishers said to be involved in an attempted hijack of the personal email accounts of WHO staffers.

3 THE INFILTRATOR

Infiltrators rely on virtual back doors and unprotected points of entry to slip through hidden cracks. Hiding in the shadows, this type of cybercriminal lurks, watches and waits for the opportunity to invade systems. DNS (Domain Name System), which is considered a trusted protocol, is especially vulnerable. Once the criminal redirects internet traffic to malicious websites or takes control of servers, the damage is inevitable. But thanks to modern technology and security awareness training, damage can be mitigated quickly.

DNS is an Unlocked Back Door

One of the most common methods of infiltration includes internet-based attacks, such as Denial of Service (DoS), Distributed Denial of Service (DDoS) and DNS poisoning. By default, DNS traffic is unencrypted, allowing internet service providers and other third parties to monitor website requests, surveil browsing habits, and even duplicate web servers to redirect traffic. However, cybercriminals can also use legal DNS traffic surveillance to their advantage. There are several examples that show the vulnerabilities of DNS:

AWS DDoS Attack
Amazon reportedly mitigated the largest known DDoS attack in history, stopping a 2.3 terabit-per-second (Tbps) threat. The attack hit the Amazon Route 53 DNS web service, impacting all AWS services and thousands of Amazon customers.[14]

GitHub DDoS Attack
Prior to the AWS attack, the largest verifiable DDoS attack on record (1.3 Tbps) targeted the web development platform GitHub. Hackers used amplification to affect the database's caching system, flooding servers with spoofed requests.[15]

The Mirai Krebs Attack
The blog of cybersecurity expert Brian Krebs was assaulted by a DDoS attack in excess of 620 Gbps, which was three times bigger than any previous attack. The source was the Mirai botnet made up of 600,000 compromised IoT devices.[16]

> "MSPs can benefit from deploying DNS protection solutions that support DNS-over-HTTPS, especially for employees working remotely on unsecured devices."
>
> **Grayson Milbourne,** Webroot

DNS Attacks Are a Threat to All Businesses

The goal of DDoS and other infiltration-based attacks varies, but disruption and financial gain are desired outcomes for infiltrators. In some cases, criminals may launch a DDoS attack on a specific business to demand a ransom payment or another action, like providing access to a network or third party, in order to restore service. They can also be launched by a rival business to discredit the victim's service and damage their reputation with customers. Around 82% of organizations have faced a DNS attack at some point, and the average cost per attack is now $1.07 million.[17]

Stopping Infiltrators with DNS-over-HTTPS

To protect against DDoS and other DNS attacks, ISPs like Google and Mozilla have been working to encrypt and secure the Domain Name System.[18] In 2018, DNS-over-HTTPS (commonly known as DoH) was proposed as the standard protocol for encrypting DNS requests. It works by preventing infiltrators from accessing the information and, in some cases, making it difficult to tell the difference between a DNS request and other HTTPS traffic.

This encryption ensures that no one can tamper with a web page while you're viewing it or spy on your browsing behavior. For example, if you connect to a website, a network operator like your ISP or a public Wi-Fi hotspot can only see the domain name of the site you're reading, not the IP address itself. This keeps your browsing secure and prevents access to cybercriminals attempting to spoof the site or launch an attack.

However, DoH isn't perfect. If all DNS requests are encrypted, then admins can lose considerable visibility and control in terms of web filtering security. When applications are capable of making DNS requests independently, it defeats the value of web filtering by circumventing the in-place protections. To correctly leverage the advantages of DoH, it's important to use the right DNS protection.

An effective solution should encrypt and manage the DNS requests for the entire system, and then securely relay these requests via DoH. This way, administrators retain control of the DNS while users benefit from the additional security.

DISRUPTION IS COSTLY

There are several types of infiltration attacks that utilize flaws in internet security to cause disruption or damage. A DoS or DDoS attack is designed to disrupt normal web traffic or make a website unavailable in some way, often used to leverage ransoms from victims.

Network flooding is a type of DDoS attack that floods DNS servers with high volumes of traffic, making the service temporarily unavailable. While not always associated with ransoms or specific financial loss, flooding and other DNS attacks can cause serious disruption to businesses of all sizes.

Even short website or network outages can increase downtime. According to Gartner, the average cost of IT downtime is $5,600 per minute.[19]

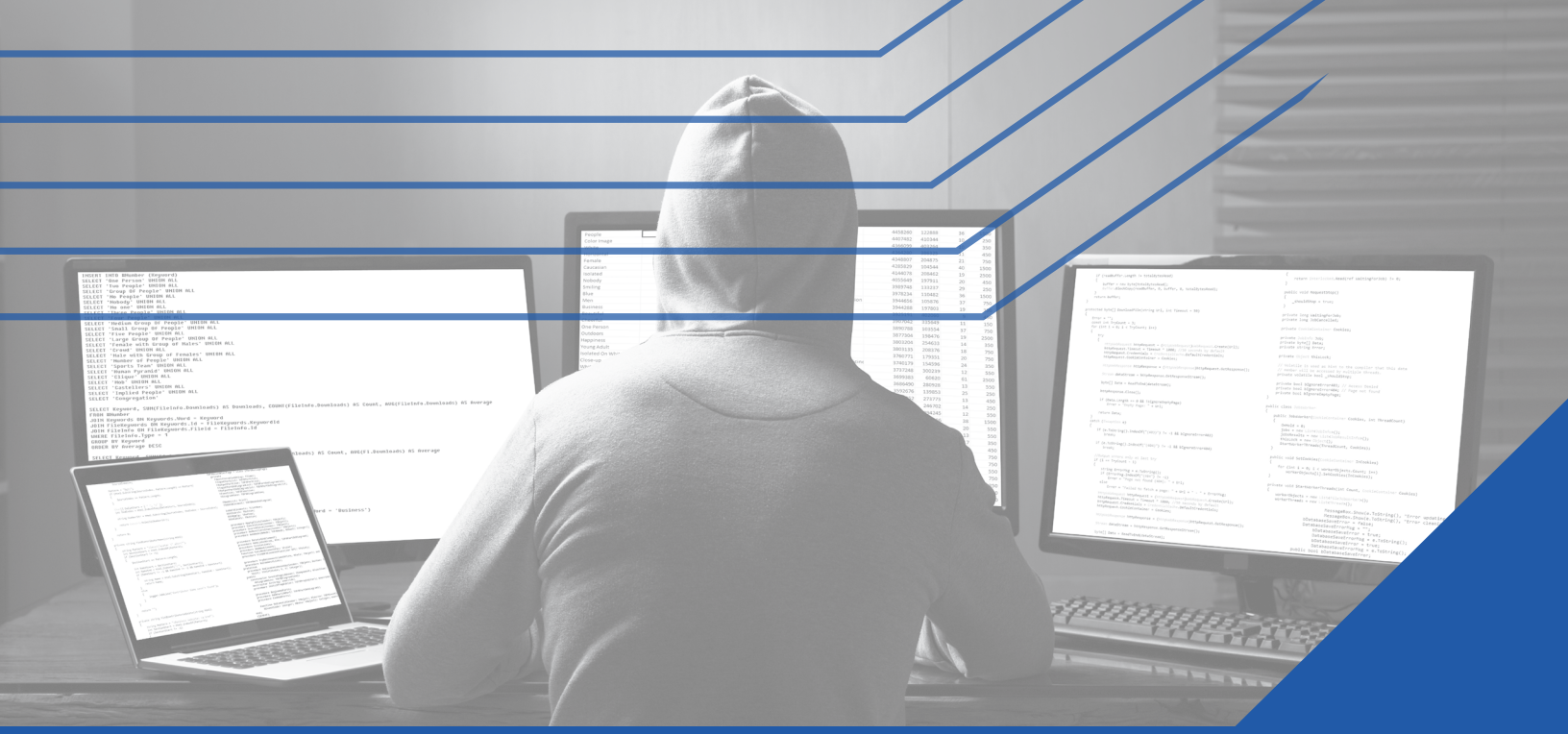
HOW TO PROTECT YOUR BUSINESS

Protecting against multiple threats requires a layered approach. On the technology side, it's imperative to use cybersecurity solutions that protect every endpoint and regularly participate in security awareness training to educate your employees and customers. Here are the top security best practices to follow:

- **Ensure every employee installs robust endpoint security on all devices**
- **Instruct employees to delete requests for financial information or passwords**
- **Warn employees to follow security best practices when opening or downloading COVID-19 related emails, links, or mobile apps**
- **Follow IT security best practices by updating and patching software and firewalls as well as network security programs**
- **Make sure to use RDP solutions that encrypt the data and use two-factor authentication and VPNs to connect to corporate networks**
- **Leverage advanced machine learning tools to automate the detection of phishing sites**
- **Keep customers safe from IP threats with predictive IP reputation services**
- **Work with your ISP to monitor any heavy traffic to your website and ensure server capacity can handle heavy traffic spikes**
- **Offer and regularly participate in Security Awareness Training and phishing simulations for employees and customers**
- **Use cybersecurity software with real-time anti-phishing services**
- **Develop an incident response plan in case of a DDoS attack**
- **Use DNS protection and leverage professional DDoS mitigation services**

Impersonators, opportunists, and infiltrators are everywhere. Secure your business and protect your reputation with world class cyberesecurity solutions from Carbonite and Webroot!

Start My Free Trial



1 CNBC, "17-year-old accused of masterminding Twitter bitcoin scam."
2 MSN, "Shark Tank star duped out of $400k in phishing scam."
3 Forbes, "Phishing Scam Costs Texas School District $2.3 Million."
4 Webroot. "Hook, Line, and Sinker: Why Phishing Attacks Work."
5 Wall Street Journal. "Fraudsters Used AI to Mimic CEO's Voice in Unusual Cybercrime."
6 Entrepreneur, "FBI Sees Cybercrime Reports Increase Fourfold During COVID-19 Outbreak."
7 Webroot, "Cyber News Rundown: Malicious COVID-19 Websites Surge."
8 Security Intelligence, "Conti Ransomware Identified as Ryuk's Potential Successor."
9 FBI, "Charity and Disaster Fraud."
10 Michigan Live, "Internet trolls spew profanity, racial slurs during first virtual Kalamazoo city meeting."
11 FBI, "FBI Warns of Teleconferencing and Online Classroom Hijacking During COVID-19 Pandemic."
12 CNN, "Beware of these fake text messages and robocalls going around about the coronavirus."
13 INTERPOL, "INTERPOL report shows alarming rate of cyberattacks during COVID-19."
14 ZDNet, "AWS said it mitigated a 2.3 Tbps DDoS attack, the largest ever."
15 GitHub, "February 28th DDoS incident report."
16 KrebsOnSecurity, "KrebsOnSecurity Hit With Record DDoS."
17 EfficientIP, "IDC 2019 Global Threat Report"
18 Encrypted-DNS.org, "Encrypted DNS Deployment Initiative."
19 The 20, "The Cost of IT Downtime."

About Carbonite and Webroot

Carbonite and Webroot, OpenText companies, harness the cloud and artificial intelligence to provide comprehensive cyber resilience solutions for businesses, individuals, and managed service providers. Cyber resilience means being able to stay up and running, even in the face of cyberattacks and data loss. That's why we've combined forces to provide endpoint protection, network protection, security awareness training, and data backup and disaster recovery solutions, as well as threat intelligence services used by market leading technology providers worldwide. Leveraging the power of machine learning to help protect millions of businesses and individuals, we help secure the connected world. Carbonite and Webroot operate globally across North America, Europe, Australia, and Asia.

Discover cyber resilience at carbonite.com and **webroot.com.**