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

HACKER PERSONAS

A Deeper Look Into Cybercrime

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 by impersonators and unsuspecting victims sent bitcoin to a specific cryptocurrency wallet with the promise of doubling the sender's investment. More than 320 transactions took place, resulting in $110,000 USD being deposited into the fake wallet.[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]

Manor, 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 known 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

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.

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.

HOW TO PROTECT YOUR BUSINESS

☑ Instruct employees to delete requests for financial information or passwords

☑ Use cybersecurity software with real-time anti-phishing services

☑ Leverage advanced machine learning tools to automate the detection of phishing sites

☑ Keep customers safe from IP threats with predictive IP reputation services

☑ Follow IT security best practices by patching software and securing email servers

☑ Offer and regularly participate in Security Awareness Training and phishing simulations for employees and customers

Protect against social engineering attacks with Security Awareness Training!

START MY FREE TRIAL

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 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.

[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."