DomainGuard

PHISHING WHITEPAPER

JULY 2021

Phishing On The Rise

Phishing continues to be the most successful tactic used by hackers to gain a foothold into an organization. Relying on unsuspecting users, phishing takes advantage of the **human layer** in security; a layer seemingly indefensible. Phishing attacks were up 41% in Q1 2021 compared to Q1 of 2020[1].

Remote Workforce

41%[1]
Phishing Increase

This spike in phishing strongly correlates with the largest remote workforce in human history. Due to the COVID-19 pandemic, many industries were forced to transition to **remote work** and as a result company resources had to be made available to this remote workforce. With employees flooding home and still needing to work, companies had to create new bridges to resources. These bridges can be accessed from the same network that many employees share with their family. Likely the same network where children and adults are gaming (rage-quitting) and smart devices are connected out the wazoo - because you just have to have the smart bulb hues that match your current mood.

Hackers or SEO Experts?

87%[1]
Legitimate Certificate

Many targets which were once inaccessible from outside the office have now become juicy targets for hackers. While this increase in overall phishing is affecting all industries, DomainGuard has noticed an increase in phishing attacks against **small businesses**, specifically **local banks**. We've seen hackers clone websites of small local banks in rural Pennsylvania to branch banks in London. The beauty of the Internet is global communication, allowing your customers to access your website from anywhere in the world. This beauty can turn ugly real quick when a hacker in another country clones your website and sends phishing emails to your employees or to attempt to dupe your customers. We've even seen phishing sites so sophisticated they were indexed in Google ahead of the legitimate site. These hackers should consider SEO (Search Engine Optimization) as a more legitimate line of work.

Ineffective Controls

Even with proper controls in place, phishing attacks continue to have great success. While organizations should always enable Multi-factor Authentication (MFA) where possible, employees continue to accept MFA requests that were triggered by an attacker. Several security consulting firms have informed us that they regularly have success with their phishing campaigns when prompting a victim to accept an MFA authorization. Unfortunately, some employees see a MFA request as a to-do as opposed to an entryway into a company asset. If it's one thing we've learned as security experts, it's that people love to click things and this same joy of clicking applies to MFA requests. Many employees do not realize the implications of accepting a MFA request not triggered by themselves.

Phishing Awareness

DomainGuard recommends companies conduct regular phishing awareness training and inform employees they will never receive a MFA request that wasn't triggered by them. Any such events should be reported to security. However, users are – primarily – human, and as such are prone to mistakes. Security awareness training is extremely important, but must be reinforced with technical solutions to help where users fall down.

Attacks Increasing Complexity

The majority of phishing campaigns we've seen in the past lack sophistication and were easy to spot, but this trend is changing. In 2021 we've seen an increase in the complexity of these phishing campaigns, the majority of which utilized valid certificates. In addition to using valid certificates, hackers utilize typo-squatting and register domains similar to an organization's domain. While they may be giving the pretense that this is simply typo-squatting and they're trying to sell the domain and hide behind a parked page, the reality is that many of these domains are being aged for use in a future phishing attack. Per discussions with local security firms: Penetration tests where a targeted, sophisticated attack is included as part of the scope have success rates of nearly 100%. This fact is alarming because it shows that even when organizations have all the proper technical controls in place, hackers can still get in by tricking an employee.

1 https://www.prweb.com/releases/phishing_attacks_increase_47_in_q1/prweb17963730.htm

Guard Your Domain

Defense In Depth

The best defense strategy which applies to all facets of security is **defense-in-depth** or a layered defense. DomainGuard acts as the Domain Monitoring layer of defense and continuously monitors for potential threats based on your domain name. As new domains are registered or certificates are issued that relate to your domains or your brand, our team of security experts will monitor these results and inform you of any potential threats. Our goal is to provide end users with **actionable security data**, and as such, DomainGuard only notifies you when a security threat has been identified by one of our security experts. You can focus on your business while we guard your domain.

DomainGuard Detection

With DomainGuard, your organization can take a proactive approach to phishing protection. We'll continuously monitor your domain for threats, and notify you when threats are identified.

Malist Threat Feed

Our threat feed, **Malist**, is a feed of all Domains and IP addresses we've categorized as threats. If a hacker is conducting a phishing campaign targeting your organization, it's likely they're doing the same for others. As the DomainGuard network grows, so will the quality and depth of our threat feed.

Grow With Us

We are a young company, made up of seasoned and experienced **cybersecurity professionals**, and have the benefit of being agile and able to adapt. We're looking to **build partnerships** with our clients and adapt our tooling to best serve the needs of our partners. We'd absolutely love the opportunity to earn your business and we encourage you to reach out. For any inquiries, please reach us via email or through the contact form on our website.

-Erkin Djindjiev,
Founding Engineer