Cyberfish White Paper

Next Generation Anti-Phishing

Phishing is the #1 One Attack Vector

Phishing is the most effective, prevalent and cheap to carry out cyber attack.

Organizations deploy multiple layers of security technologies to prevent, detect, and respond to cyber threats. But even with these controls in place, organizations are still far more likely to be compromised via a phishing attack than any other attack method.

These attacks used to steal finances, extort ransom payments, exfiltrate intellectual property, disrupt business operations and, in many cases, can put a company out of business.

Your Company Is Targeted, But You're Not Protected

76% of businesses reported being a victim of a phishing attack in the last year*, while 95% of all attacks on enterprise networks are the result of successful spear phishing**.
According to Symantec, phishing rates have increased across all industries and organization sizes — no company or vertical is immune.

Today's email security and web gateway solutions such as Symantec, Forcepoint and Proofpoint offer basic phishing protection based on outdated blacklist technology, able to detect less than 10% of potential attacks. Advanced gateways such as CheckPoint and Barracuda improve detection by using endpoint data, but still fail to address most of the spear-phishing and impostor attacks.

Another approach which is employees training is important, but requires a lot of effort from the IT department and shows only a partial decrease in phishing email click rate.

On Nov 2018, The U.S. Securities and Exchange Commission recommended to all public companies to consider cyber threats such as a phishing and Business Email Compromise (BEC), when implementing internal accounting controls.

---

* – Wombat Security State of the Phish
** – SANS Institute

Zero-Hour Detection

Cyberfish is The Next Generation Anti-Phishing solution that combines Computer Vision and AI to detect phishing emails and pages in real-time.

Cyberfish prevents zero-hour attacks by detecting new, just created, phishing websites and impostor emails, drastically increasing the detection rate to an unprecedented level.

Holistic Anti-Phishing Solution

Cyberfish is one-stop defense solution for all phishing-related attacks, such as spear phishing, scam, impostor emails (CEO fraud) and malware/ransomware delivered via links.

➤ Real-Time Detection

Cyberfish detects new, just created, phishing and fraud websites which lead to credential thefts pages or malware. Cyberfish is the only solution that also discovers mediator pages containing phishing and malware links, which are created to fool security gateways.

➤ Sender Analysis

Cyberfish automatically detects impostor and fraud email whether sent using spoofing or address impersonation, utilizing several techniques, including visual analysis of email assets.

➤ Document Scanning

Cyberfish scans email attachments and detects links hidden in attached documents (PDF, MS Office, text files, cloud documents) which point to phishing websites and malware.

➤ Employee Training

Integrated with our top-notch detection engine, Cyberfish offers optional training module, which continuously builds employees phishing awareness by sending relevant, real-data simulation emails with contextual data based on undergoing attacks.

One-Click Integration

Cyberfish is a non-proxy solution with non-brainer deployment and low-touch support.

Cyberfish is integrated with popular email cloud providers such as Google Gmail and G Suite, and Microsoft Office 365 family (Exchange Online | Office 365), as well as with MS Exchange with On-Premise deployment.

Cyberfish also offers powerful URL phishing detection API, as well as OEM solutions.

How Cyberfish Protection Works

Cyberfish stops spear phishing, malware links, and impostor (CEO fraud) by making a paradigm shift in email analysis approach. Cyberfish uses a unique combination of several technologies.

✦ Brand Monitoring

Cyberfish proactively index and monitor top brands assets, as well as phishing kits, and use a combination of AI and Computer Vision to detect impersonation. Adding custom brands takes less than 5 minutes.

✦ Visual Analysis

Cyberfish uses computer vision to analyze the visual representation of each scanned email and link opened in a real browser, as well received email metadata such a sender name and email address.
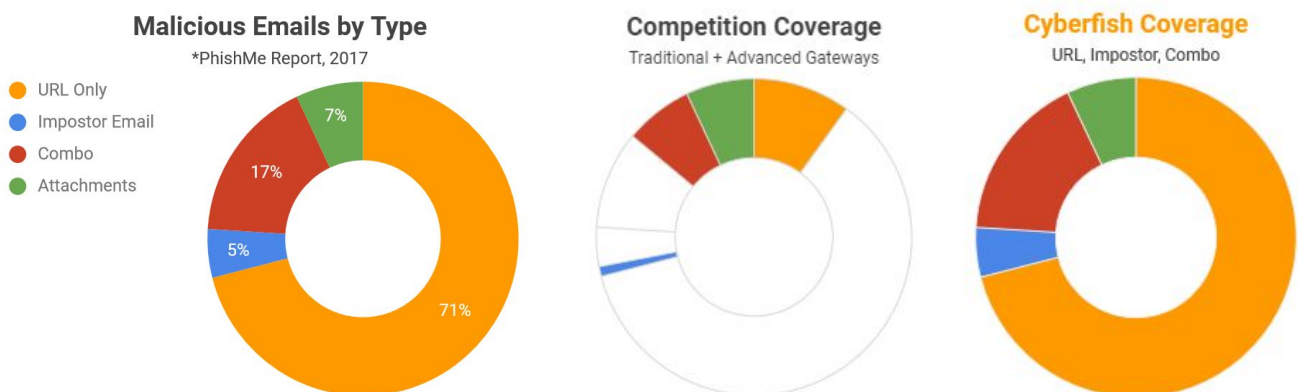
✦ Multi-Source Detection

Due to unique technology of opening emails and links, Cyberfish traces all redirects, including browser side ones. Cyberfish also discovers malicious links hidden in email attachments such as PDF or cloud-based documents, as well as text links.

✦ Smart Blacklists

Combination of existing and proprietary URL whitelists and blacklists is being used to enhance phishing detection, in addition to our unique visual blacklist technology.

Cyberfish technology is patent pending.

Cyberfish Protection Coverage

Malicious Emails by Type
*PhishMe Report, 2017

- ● URL Only
- ● Impostor Email
- ● Combo
- ● Attachments

71%, 5%, 17%, 7%

Competition Coverage
Traditional + Advanced Gateways

Cyberfish Coverage
URL, Impostor, Combo

Benefits and Advantages

Cyberfish core advantage is the ability to "look" at emails and websites from an end-user perspective and stop the attack in real-time before it has been reported. Cyberfish adds a must have an extra layer for the security of organizations and allows fast, low-touch integration which does not require changes in company's current network landscape.

✔ Focus on Phishing

Cyberfish focuses specifically on all types of phishing-related attacks, such as spear phishing, impostor email, and ransomware. Cyberfish protects email not only on the desktop, but also on any mobile device.
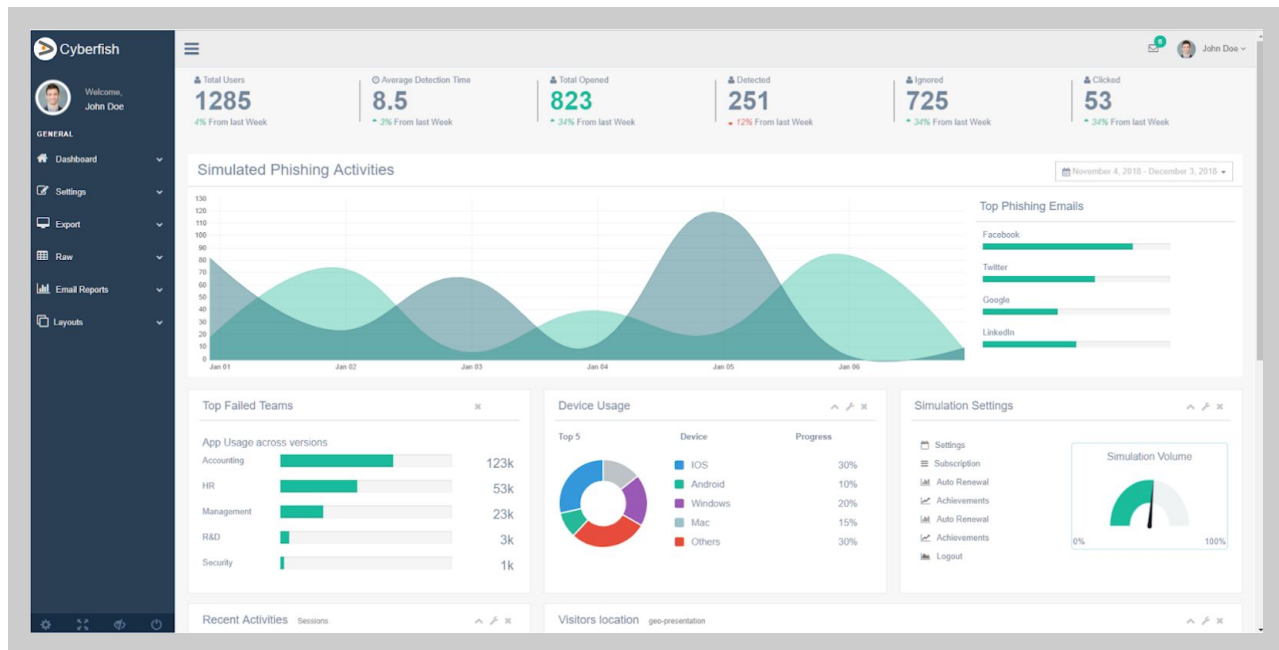
✔ Zero hour protection

We protect you when it matters first - most successful attacks happen within 24 hours after setup of new phishing page and rolling out a phishing attack.

✔ Simple, Non-Proxy Integration

Cyberfish is easily deployed in cloud or on-premise while sitting next to mail server infrastructure and not interfering with current network setup.

✔ Effective Training

Our training module does not require manual setup of campaigns, but in the same time continuously delivers targeted phishing simulation emails. Cyberfish "Report a Phishing" button is available both on desktop and mobile, closing the loop between protection and awareness.

Dashboard & Reporting

Cyberfish offers a simple configuration interface, as-well-as interactive dashboard which with both live and periodic reports, including reports specifically designed for company's executives.

About Cyberfish

Cyberfish is a company consists of some of the top experts in email and security. We believe that web should be a safer place. We have seen companies destroyed and people life ruined because of phishing and fraud attacks. We want to stop it.
We focus on bringing our solution to mid-tier and enterprise companies, who suffer from phishing attacks the most. Contact us at team@cyberfish.io