

FraudWatch Anti-Phishing



Protect your enterprise brand, establish trust, and reduce losses.

Phishing – Reduce the criminals Return on Investment

Phishing has become a popular method of identity and credential theft, and has targeted financial, ecommerce, ISP, auction and social networking websites. Any enterprise with an online presence is at risk from phishing, which leads to brand damage, erosion of customer confidence in the online channel, financial losses and increases customer care costs.

The sophistication of phishing scams continues to increase with RockPhish and fast flux DNS methods, making the fight against phishing increasingly difficult and prolonging the duration of each phishing attack, increasing financial returns for criminals, and losses for enterprises.

The key to fighting phishing from an enterprise perspective is to make your company a difficult target, reduce criminals return on investment, and encourage them to target their activities elsewhere. An effective Anti-Phishing Solution will achieve this result through proactive monitoring and fast site take down services.

FraudWatch Anti-Phishing

FraudWatch provides a comprehensive end to end solution to mitigate and eliminate phishing incidents quickly. The solution includes proactive monitoring and detection of phishing incidents, through to the rapid site take down response and resolution of the incident.

Our always-on phishing monitoring & detection engine receives inputs from honeypots, spam feeds, client abuse email and other data sources. This removes duplicates and provides an early warning system for phishing URL's targeting a specific brand. Our DNS and domain registration monitoring provides the ability to prevent a phishing attack before it begins, alerting to similar domain registrations to those of our clients brand.

FraudWatch maintains a 24x7 Security Operations Centre, fully staffed with Security Analysts who specialise in phishing analysis and incident take down. Relationships have been built with ISP's and Web Hosts around the world to facilitate in timely site take downs. Our analysts work a number of contact channels simultaneously, (including ISP's, Web Hosts and Website owners/administrators) to ensure each phishing incident is taken down in the fastest possible time.

Our Phishing Reporting & Forensics portal provides a central location for incident reporting, data repository for all forensic data relating to each incident, including domain and IP whois data, website source code, phishing email and headers and any other associated files gained during the incident response. The portal also provides a comprehensive reporting view of individual and incidents and trends.

FraudWatch Anti-Phishing provides clients a comprehensive solution to mitigate the impact of phishing incidents, reduce brand damage, maintain customer trust in the Internet channel, and minimize fraud losses.

Mitigate Phishing
Attacks with Fast
Site Take Downs.

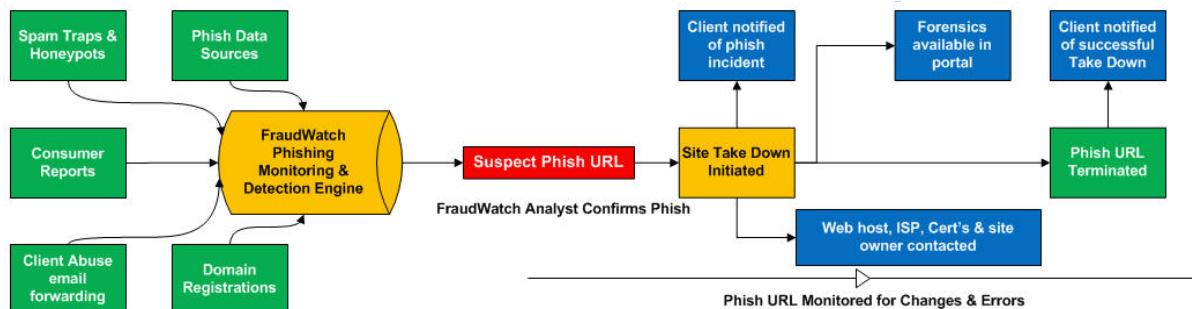
FraudWatch
provides the
fastest site take
down possible
through
established
global
relationships

Datasheet: FraudWatch Anti-Phishing

FraudWatch Anti-Phishing Features

- **Proactive Monitoring** of various sources for phishing attacks targeting your brand, including honeypots, spam feeds and other phishing data sources.
- **Domain Monitoring** provides early detection of similar domain registrations to thwart an attack before it begins; DNS servers and new domain registrations are monitored.
- **Abuse Email Forwarding** from your customer abuse email directly to FraudWatch for analysis, de-duplication, and verification of a new attack.
- **Evaluation & Verification of potential phishing threats** by FraudWatch Security Staff, and verified prior to initiating a site take down response.
- **Rapid Response & Site Take Down** using our worldwide relationships with ISP's, Web Hosts, CERT teams and Law Enforcement.
- **RockPhish and Fast Flux domains** are easily managed by shutting them down at the registrar level through our relationships with domain registrars.
- **Continuous Monitoring of phishing URL's** by FraudWatch systems to alert of content changes, IP changes and take down. Monitoring continues for 180 days after site take down.
- **Reporting & Forensics Portal**, providing a central location for incident reporting and phishing incident data repository for all forensic data, which also provides comprehensive reporting.
- **URL inclusion in Global Blocklists**, through FraudWatch's relationships, URL's are included in popular browser and other blocklists, protecting users from visiting known phishing sites.

FraudWatch Phishing Incident Detection & Response



FraudWatch Security Analysts work tirelessly to ensure each phishing site is taken down as fast as possible, often working through multiple communication channels simultaneously.

Phishing incident forensics are made available to clients as soon as the URL is analysed and confirmed as a phishing incident. Incident forensics remain available post incident, for as long as the client remains within an active contract with FraudWatch.



Datasheet: FraudWatch Anti-Phishing

Frequently Asked Questions

How does FraudWatch define a phishing incident?

FraudWatch's basic definition of a phishing incident is a unique IP and URL combination. Some phishing websites will be taken down on one host, only for the domain to be moved to another host, which requires an entirely new take down effort.

Some phishing URL's may be grouped together in one incident if they are on the same domain name, simply in different directories (not sub-domains) and are active at the same time.

Example: www.phishsite.com/banking/update/index.htm will be grouped together as 1 incident with www.phishsite.com/abcbank.com/update.htm

A Phishing URL is active if it can be accessed live on the Internet. The URL is inactive and the incident is closed if the URL can no longer be accessed on the Internet.

A Phishing incident is considered closed after the site has remained inactive for 30 days. If within 30 days of a site being taken down, it becomes active again, the original incident is reopened. If the site becomes active again after 30 days, a new incident is created.

Does FraudWatch offer a phishing site take down time SLA?

Every phishing incident has different characteristics, including where it is hosted, if there are 3rd party web hosts involved, and if the website administrator contact details are current. Some phishing incidents will be taken down within 10 minutes, whilst others can take several hours, or in extreme cases, several days.

As such, FraudWatch does not offer SLA's on site take down services; however, rest assured that our experience and global relationships allows us to provide the best possible site take down results. Our Security Operations Centre analysts work tirelessly to do all we can to have every phishing incident resolved in the fastest possible time.

What is Vishing and how does FraudWatch handle this threat?

Vishing uses Voice over IP (VoIP) to impersonate a Financial Institutions Telephone system, and is used to gain access to the customer's financial information. Customers are lured into calling a VoIP phone number from an email, SMS or voicemail. Vishing is very difficult for authorities to trace, but the service can be terminated.

When a vishing incident has been identified with a phone number, FraudWatch will work to have the phone number terminated. This is not as simple as a standard phishing incident, and does take more time and effort.

Why FraudWatch:

- **FraudWatch specializes in Anti-Phishing**
FraudWatch provides unique expertise within the Anti-Phishing Industry, being one of few companies to focus solely on providing Anti-Phishing solutions to the wider Internet Community.
- **FraudWatch is Flexible to meet your needs**
FraudWatch can provide personalised and flexible service at a lower total cost. FraudWatch minimises bureaucratic roadblocks to ensure each customer's individual needs are met.
- **FraudWatch maintains a 24x7 Security Operations Centre**
FraudWatch maintains a fully redundant Security Operations Centre in multiple locations. This is manned around the clock with trained staff analysing and responding to phishing incidents as they occur.
- **FraudWatch can provide a total lower cost solution**
FraudWatch provides a cost effective method of managing and mitigating the risks of phishing on a 24x7 basis, allowing your staff to focus on their routine tasks. Lower costs are translated through reduced staffing, equipment and maintenance costs.
- **FraudWatch offers a Scalable Solution**
FraudWatch provides a comprehensive solution scalable to any number of phishing incidents your company is attacked with.
- **FraudWatch can overcome Language Barriers**
FraudWatch maintains relationships with interpreters servicing over 100 languages, overcoming any language barrier to have phishing sites taken down.
- **FraudWatch is a respected partner with Global Relationships**
FraudWatch has built global relationships with, and are well respected by ISP's, Web Hosts, CERT Teams and Law Enforcement. These relationships allow for faster site take down responses through increased co-operation.



How does FraudWatch handle RockPhish & Fast Flux?

RockPhish and Fast Flux Phishing attacks involve a large number of newly registered domains, all pointing to a rotating list of IP addresses on a botnet, often in the thousands. The best way to handle RockPhish and Fast Flux attacks is to have the domain deregistered, which, depending on the domain registrar, can take longer than a standard phishing incident. FraudWatch works with domain registrars around the world to have domain deregistered as quickly as possible.

RockPhish attacks can involve anywhere from 100 to 500 domains over the course of a 2 week attack. The registrar of each of those domains must be contacted in each instance. Some financial institutions do not peruse RockPhish domains due to the enormity of the attack, however FraudWatch has successfully had a number of clients removed from the RockPhish kit – purely because we are proactive and let the criminals know it – they move on to easier targets who will not continue to have their domains deregistered.

About FraudWatch

FraudWatch International, a privately owned Internet Security company established in 2003 has Global Sales Offices, and has its headquarters in Melbourne, Australia. FraudWatch's core business is 'phishing fraud prevention', providing a variety of anti-phishing products and services to protect consumers and business and currently protects over 200 million Internet users worldwide.

FraudWatch uniquely focuses on phishing fraud. Although other Internet Security companies recognise phishing as a security threat, most regard phishing as secondary to their core business.

We report the latest detected phishing incidents daily, providing the largest list of phishing incidents available on the Internet today.

Our Security Operations Centre provides 24x7 phishing monitoring, detection and site take down services.

The Internet community, including ISP's and Financial Institutions respect and appreciate our work in the fight against phishing.

FraudWatch International Pty Ltd
ACN: 109 760 796
Level 1, 234 Whitehorse Road,
Nunawading 3131 VIC Australia.
GPO Box 3537 Melbourne 3001 Australia
Tel: +613 9759 7219
Fax: +613 8660 2688
Web: www.fraudwatchinternational.com
sales@fraudwatchinternational.com



Datasheet: FraudWatch Anti-Phishing