

C·O·M·O·D·O Anti-Phishing Portfolio

PREFACE

Phishing is the fastest growing threat in the history of Internet and has gained immense popularity amongst Internet fraudsters and hackers as a simple yet effective way to gain unsolicited access to confidential user information. Using social engineering tactics, fraudsters ensure that the trust relationship established by a company with its customers is exploited to maximum effect. Emails that pose to have originated from credible sources instigate customers to hand over sensitive data via forms on spoofed web sites. The simplicity by which HTML, and graphics can be cut and pasted from e-mails and web pages means a virtual perfect replication of the legitimate versions, thus leaving minimal opportunity for the victim to escape this malicious attack.

The simplicity by which credit card fraud and identity theft is undertaken is evident in the fact that such attacks are growing both in numbers and in complexity. With Phishing attacks now being launched on a global base, not only does it endanger the interest of the end customers but also poses a significant threat to the reputation of online business.

THE HARD FACT

It is the responsibility of the business community to ensure appropriate control measures are taken at every level to mitigate the threat and drive out the potential for profitability and gain. If not then the remediation costs stand to be far higher with users losing confidence and the online business losing customers.

COMODO ANTI PHISHING PORTFOLIO - OVERVIEW

Comodo have taken a proactive approach in identifying and combating the threat of identity theft with a portfolio of synergistic solutions.

The Comodo Anti-Phishing portfolio is a combination of tools and services to equip organizations with a comprehensive defense strategy and control architecture to fight the Phishing threat at all levels including gateways, across web servers and through end users. The core portfolio leverages preventive, detective and corrective actions responses across multiple levels.



PREVENTION

Content Verification Certificates (CVC)

Content Verification Certificates (CVCs) facilitate the verification of "web page content". As an X509 compliant certificate type, CVCs are created, distributed, and revoked using proven PKI (Public Key Infrastructure) methods to provide the highest level of security for web page content. Facilitating the deployment of verified login boxes, verified navigation panes, verified trade marks / brands and verified accreditation/association logos. Combined with freely distributable tools like VEngine™, CVCs empower enterprises to take a proactive preventative response to Phishing attacks. Protecting the content of a web page and allowing verification.

For content to become 'verifiable' by the user it must be:-

- 1) Suitably complex such that it cannot easily be spoofed (No cut and paste possibilities)
- 2) Directly linked (bound) to the web page (URL and or IP) upon which it is to be displayed
- 3) Given a validity period related to its usage.

'VerificationEngine' the patented browser plug-in for Internet Explorer from Comodo allows users to verify that a digitally signed element of content can exist on an approved web page. For example, which website below is legitimate and which is not?



Web Site 'A'



Web Site 'B'

A verification process (A process that is initiated by the user and not the web server) allows any digitally signed content bound to a specific URL/IP to be rendered onto the display in a different way to all other 'non verified elements, easily highlighting trusted elements. So in the example of the web site above, the 'real' web site would display trusted elements highlighted, where as the 'spoofed' site would not be able to and would display all elements as 'un-trusted'.



Web Site 'A'
FALSE



Web Site 'B'
REAL



C·O·M·O·D·O Anti-Phishing Portfolio

High Assurance Secure Socket (SSL) Layer Certificates

A SSL encrypted session between web browser and the web server provides a secure tunnel but does not necessarily provide assurance of the identity of the end entity. Whilst a few high assurance providers continue to offer high assurance validation processes, many more low assurance providers are entering the market offering automated validation procedures. With no capability for the browser to differentiate between brands of SSL provider blanket trust is established to the detriment of the browser user. Only in-depth analysis of Certificate Authority Practice statements can provide the necessary guidance and advice. In most cases this is impractical for a browser user. Comodo therefore offers solutions which provide simple and effective differentiation for the user. With browser users given the power of choice, enterprises have a responsibility to ensure that the use of high assurance SSL certificates provides customers the identity assurance and confidence to make safe, secure on-line transactions.

TrustLogo™

TrustLogo™ removes a major barrier to successful e-commerce: the lack of the ability to verify the trust between a website and its visitors. Powered by the Internet's only real-time Identity Assurance infrastructure IDAuthority™, TrustLogo delivers trust, confidence and peace of mind to customers.

TrustLogo provides a unique ability to visibly display the "trusted" and "secured" status of an enterprise and essential business credentials in real-time.

EPKI (Enterprise Public Key Infrastructure)

Corporate identity theft presents a major threat to any sizeable organization. Operating an unsecured mailing solution not only opens the organization to identity theft; it does not provide any simple and effective means of encryption, confidentiality and integrity. A simple and effective web based PKI solution from Comodo EPKI Manager provides a means to ensure the identity of the internal corporate users but it also builds a higher level of confidence and trust with communications to external customers.

Email Certificates

As spam remains the most prolific Phishing transport mechanism the inability of a user to identify the correct source of the Email (Email "From" addresses are very easy to spoof) provides no assurance mechanism. Both organizations and individuals are vulnerable to such threats. Email Certificates digitally sign or encrypt e-mail to provide that level of confidence.

HackerGuardian™

Vulnerability scanning services ensure servers and websites remain free of vulnerabilities as well as both known and unknown exploits. Visible real-time certification is available to customers providing increased assurance and trust. Comodo's managed security assessment services assist enterprises in securing their front end services.


Comodo
US Headquarters
525 Washington Blvd, Jersey City,
NJ 07310, USA
Tel Sales: +1 800 772 5185
Fax Sales: +1 646 442 3760
Canada Tel Sales: +1 877 80 32 556
sales@comodo.com


Comodo
EMEA Headquarters
New Court, Regents Place, Regent Road
Manchester, M5 4HB, United Kingdom
Tel Sales: +44 (0) 161 874 7070
Fax Sales: +44 (0) 161 877 1767
sales@comodo.com

DETECTION

Trustix Anti Spam

With the most effective mechanism of distributing identity theft attacks spam analysis and detection remains one of the foremost fronts on which Comodo operates. Trustix AntiSpam employs a combination of detection mechanisms including but not limited to real time databases, user and Trustix™ black/white lists, lexical analysis and intelligent content filtering engines. These help to identify, classify and deal with spam thereby removing potential Phishing attacks even before they are delivered to mail servers.

Trustix AntiSpyware, AntiVirus & Personal firewall

Phishing threats are commonly blended with other attack vectors to infect users machine with malicious content. The portfolio of solutions within the Trustix Security Center range scan and monitors endpoint (desktop) processes and are therefore capable of finding and deleting all known types of Trojans, worms, scripts and other harmful viruses, many of which are now beginning to launch Phishing attacks.

TrustTool bar™

TrustToolbar™ is a simple and highly effective Internet Explorer enhancement. It provides real time assurance of website identity via a trusted third party database - IDAuthority. In removing the doubt of whether a website is legitimate or fraudulent Trusttoolbar together with VEngine and TrustLogo provides the most effective and complete heterogeneous portfolio of solutions from any provider. Other advance features include verified site credentials, card payment acceptance indication; protection against URL based obfuscation (hiding) techniques and enhanced site navigation tools.

VerificationEngine™

VerificationEngine for Internet Explorer enhances the capabilities of the ubiquitous Internet Explorer web browser to that of a true trusted business tool - verifying SSL connectivity protecting the browser toolbars whilst at the same time extracting and displaying the contents of any valid CVCs.

RESPONSE

Phishing Reporting/Response Services

As a provider of critical Internet security services Comodo's Phishing Response Team (PRT) monitors and assists enterprises in detecting security issues, cases of trademark infringement and highlighting instances of potential identity theft. Feedback mechanisms have been created to update detection tools and to develop additional proactive protection solutions.

CVC - Content Verification Certificates

- <http://www.contentverification.com>

Vengine - Verification Engine - High Assurance SSL and CVC viewer

- <http://www.vengine.com>

Trustlogo - Real time web site identity assurance for businesses

- <http://www.trustlogo.com>

TrustToolbar -Real time web site identity assurance for consumers

- <http://www.trusttoolbar.com>

IDAuthority - Mapping the physical world to the virtual world

- <http://www.idauthority.com>

SSL - High Assurance SSL/TLS web server certificates

- <http://www.enterprisesssl.com>

Security - Security solutions, cryptographic/encryption solutions

<http://www.comodo.com>

Anti Virus - Endpoint Security - AntiVirus, AntiSpam, Firewall

- <http://www.trustix.com>