CLOSING THE WINDOW ON LOSSES TO PHISHING

Phishing is increasingly expensive and painful as cybercriminals find new ways to fool consumers and cash out stolen login credentials.

01 PHISHING BY THE NUMBERS

THERE WERE MORE THAN **200,000** PHISHING ATTACKS WORLDWIDE IN 2012[a]

a APWG Global Phishing Survey, 1H2012 & 2H2012

150,000+
unique domain names were used

Phishing sites are typically live for more than 10 hours

MORE THAN **600** INSTITUTIONS WERE TARGETED[b]

- Banks
- e-commerce sites
- Social networks
- ISPs
- Government tax bureaus
- Online gaming sites
- Postal services
- Securities companies

b PayPal is the most-targeted institution

More than 30 billion spam messages are sent every day

c Symatec

02 THE COSTS OF PHISHING

THE COST OF ONLINE FRAUD AND THEFT IS ESTIMATED AT **$70.2 BILLION** ANNUALLY

IMMEDIATE

Money reimbursed to compromised accounts

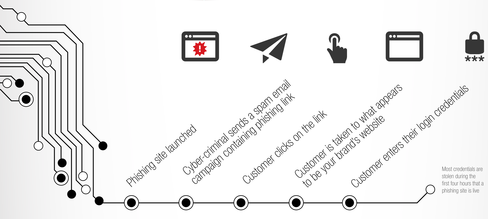
Fees paid to takedown vendors

LONG-TERM

Customer alienation

Brand erosion

03 TYPICAL PHISHING TIMELINE



Most credentials are stolen during the first four hours that a phishing site is live.

04 TACKLING PHISHING

INTELLIGENCE-BASED APPROACH -> PROACTIVE

An intelligence-based process employs techniques honed over years of research and data collection

1. **Identify suspicious sites** — Discovers hundreds more phishing sites each day than are otherwise known
2. **Verify as phish and determine brand spoofed**[d] — Prompts communication directly to your takedown vendor for quick removal of malicious content
3. **Collect digital evidence** — All links and files are extracted and analyzed in real-time
4. **Correlate the big data** — Discovers how each phishing site is linked to other phishing sites
5. **Learn to recognize future sites**

THE OLD WAY -> REACTIVE

1. Suspected phishing website is reported to you
2. You notify your takedown vendor
3. Takedown vendor confirms site is fraudulent
4. Vendor initiates takedown process
5. Fraudulent website is successfully removed

Several minutes to hours may pass between steps 4 and 5

6. Cyber-criminal launches a new site
7. The process repeats

d Process developed by world-renowned phishing experts at the University of Alabama at Birmingham

MALCOVERY SECURITY

Malcovery's intelligence-based approach to phishing reduces fraud losses and incident response costs, both near-term and in the future.

An intelligence-based response to phishing includes forensically-sound collection, data correlation, and threat research of:

- Cybercriminals' Internet location (URL and IP)
- Email addresses that are receiving stolen credentials
- Whois and reputation information about the domain name and IP
- Copies of all the component files of the phishing web site

A proactive solution offers you:

- Inside access to a valuable data mine of phishing intelligence
- The ability to search on suspicious URLs, domains, and IP addresses
- Insight into how the same threat is affecting other targeted brands
- Expert advice on referring cases to law enforcement

Saves Time
Saves Money
Protects Brand Reputation
Increases Customer Satisfaction
Increases Customer Loyalty

Contact us
Phone 855-625-2683
Email sales@malcovery.com