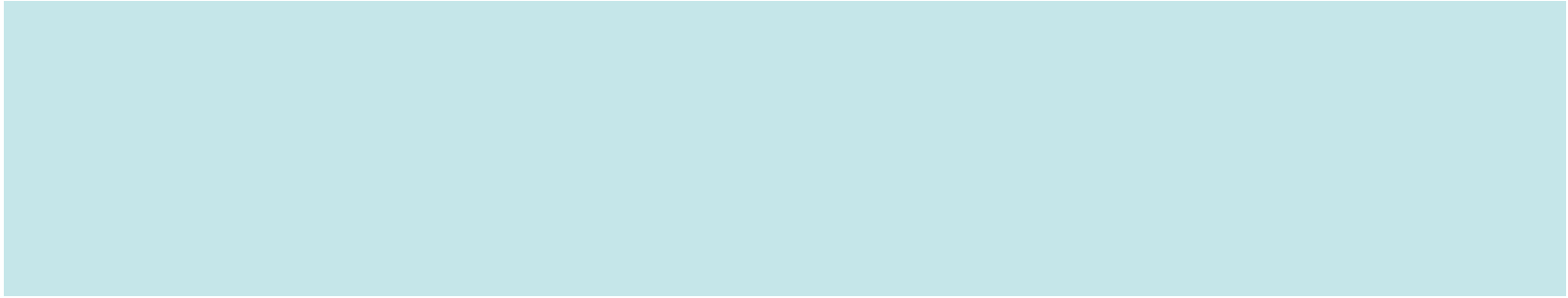




Registrar Impersonation in Phishing Attacks

Dave Piscitello, ICANN
dave.piscitello@icann.org



What is Registrar Impersonation?

- A phishing attack
- The attacker impersonates a registrar
- The phish emails are sent to
 - The registrar's customers (bulk)
 - A particular, targeted customer (spear phishing)
- Why impersonate a registrar?
 - Lure a customer into disclosing domain management account credentials
 - Use the credentials to impersonate the registrant

Why impersonate registrants?

- Malicious activities (attack the registrant)
 - Alter contact information to abet domain hijacking and business disruption
 - Alter or add mail exchange, IPv4 or IPv6 resource records to abet malicious redirection or flux phishing attacks
- Reconnaissance
 - Access information that is not published
- Facilitate subsequent attacks
 - Use credit or billing information associated with the account to purchase additional domains to use in attacks

One form of registrar phishing

- **Host the deception** (impersonate the registrar)
 - The attacker hosts a convincing duplicate of the registrar's customer portal (domain account login page)
- **Acquire targets**
 - Gather contact email addresses for the domain names (thank you, WHOIS...)
- **Lure** targets to the deception site using phish email
 - The email appears to be from the registrar *and*
 - Is **alarming** or conveys a sense of **urgency**
- **Wait** for the registrar's customers to
 - Fall prey to the lure, visit the deception site, and disclose login credentials
- **Steal** the customer's account credentials

What lures do phishers use?

- Message body is an **expected** correspondence from a registrar:
 - Domain name renewal notices, transfer notices, or order confirmations
 - Registration request confirmations
 - Registration and DNS information change confirmations
 - WHOIS accuracy reminders
 - Notices of domain name expiry or cancellation
- Message is often **personalized** to enhance the deception

Example (text ASCII)

THANK YOU FOR YOUR ORDER

Wednesday, October 19, 2005 5:18:34 AM

Dear customer,

Thank you for ordering from <registrar>.

Here are the details of your recent transaction with us. Please save this information for future reference.

CUSTOMER NUMBER: 123456789

RECEIPT NUMBER: 298884-3340

ORDER TOTAL: \$19.99

CUSTOMER SERVICE: 800-555-1234

You must login to your account to complete this transaction. Please visit the following confirmation link at <http://www.<registrar>.tld/login>

Personalized
information – does
not have to be
accurate, only
convincing

Example (HTML, hidden tag)

Dear Valued Customer,

This is a confirmation that the password for your registrar.<tld> account, mydomainaccount, has been successfully changed.

If you feel an unauthorized party has changed the password of your account, please contact Customer Support by submitting a request online at

<http://help.registrar.<TLD>/cgi-bin/php/enduser/ask.php>

or contact us at +1(888) 555-1212 .

If you have any further questions about this process and wish to consult with a Customer Service Representative contact us by submitting a request online at

<http://help.registrar.<tld>/cgi-bin/php/enduser/ask.php>.

Thank you for choosing registrar<tld>.

Customer Support <http://help.registrar.<tld>>

Hover over the
hyperlink...

How Registrars can reduce the risk

1. Only include information necessary to convey the desired message in customer correspondence.
2. Avoid using hyperlink references in correspondence with customers.
3. Warn customers against clicking on hyperlinks included in any correspondence.
4. Raise awareness that registrars are attractive candidates for impersonation.
5. Implement a form of email non-repudiation of origin for customer correspondence, such as a digital signature.
6. Implement multi-factor authentication for high-value, high security-minded domain registrants.
7. Use Extended Validation (EV) certificates for high assurance SSL connections for all sensitive transactions.
8. Provide ways to report suspected phishing attacks.

Customers: avoid being phished!

1. Do not click on hyperlinks included in email messages.
2. Use anti-spam and antiphishing features.
3. Use an email client that reveals hyperlink references.
4. Be suspicious of emails that claim an urgent response is required
5. Read email message bodies carefully.
6. Do not trust an email simply because it is personalized.
7. Verify the login form you are using is legitimate before you submit account credentials.
8. Make certain the page you visit is secured using SSL.
9. Use a unique password for your account and change it regularly.
10. Choose a registrar that requires a credit card CVV for purchases.
11. Registrants with high-value domain portfolios should consider premium services from registrars that offer additional security and monitoring measures.

More information

- SAC 028, Advisory on Registrar Impersonation Phishing Attacks (26 May 2008)
- Available in
 - English
 - Français
 - Русский
 - العربية
 - 中文
- PDFs can be downloaded