Dear Valued Customer,

There is a new phishing attack in circulation where attackers are maliciously registering fake domains that look identical to real domains by exploiting internet browsers' vulnerabilities. These fake domains can be used in phishing attacks to fool users into signing into a fake website, thereby handing over their login credentials to an attacker.

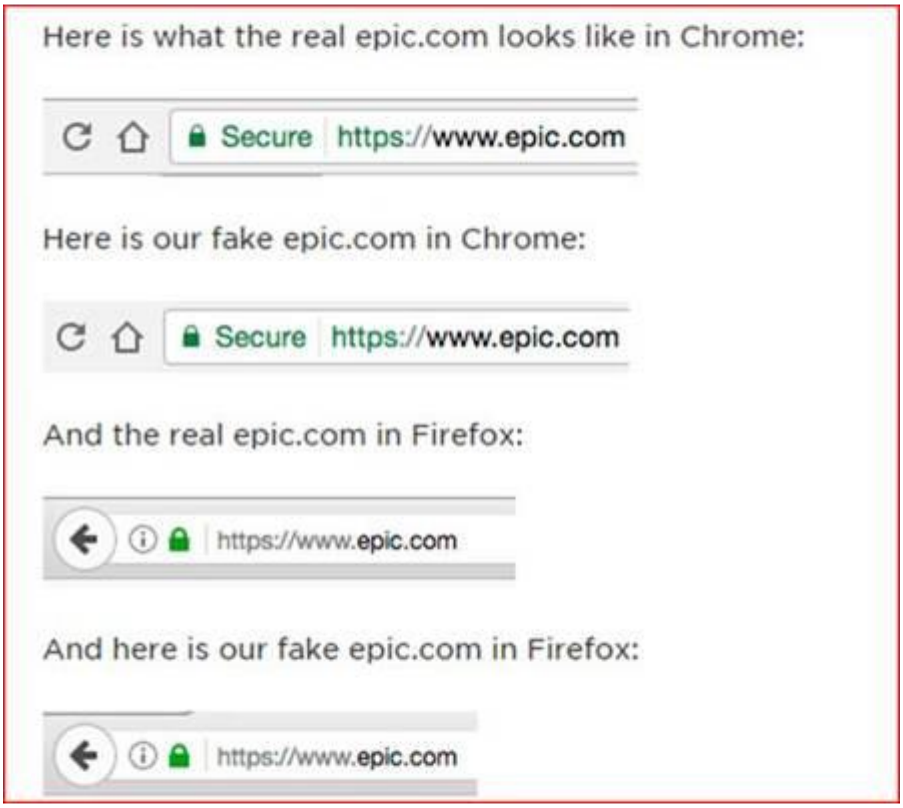
Of note, Phishing is an attempt to lure recipient(s) to share sensitive information to fraudsters (e.g. Usernames, Passwords, Credit Card details) or act upon the content, such as Funds' Transfer, by pretending to be a trustworthy individual or entity in an email for their personal gain. Whaling is another type of phishing attack impersonating senior executives and high profile individuals within institutions and banks that appear similar to genuine email.

Impacted Web Browsers

Chrome browser version 57.0.2987 and Firefox version 52.0.2.

Sample

Example to demonstrate how an attacker can register their own domain that looks identical to a healthcare official website www.epic.com.



Here is what the real epic.com looks like in Chrome:

Secure https://www.epic.com

Here is our fake epic.com in Chrome:

Secure https://www.epic.com

And the real epic.com in Firefox:

https://www.epic.com

And here is our fake epic.com in Firefox:

https://www.epic.com

Behind both fake URLs that look identical to the health care website, the attacker's actual website is hidden, i.e. https://www.xn--e1awd7f.com/

Recognising Phishing & Whaling - They often….

- create a false urgency requiring a quick response
- insist on a call to action – urge you to click a link or reply with information
- request sensitive personal information
- request not as per sender's usual transaction pattern
- contain grammatical mistakes
- request for credentials due to systems maintenance

Recommendations

- Internet Banking Users should ALWAYS access SBM Internet Banking from SBM official website ONLY i.e. through https://www.sbmgroup.mu and by clicking on the Internet Banking link on the website.

- Utmost care should be exercised while attending emails to ascertain the authenticity of both the sender(s) and genuineness of request(s). For any payment / transfer instructions, recipients need to strictly abide to the call back procedures before executing the transaction(s).

- For any suspicious emails, recipients are requested to follow the existing procedures and call back their respective clients or potential senders to ascertain genuineness of requests prior to proceeding.

- Bank will never ask for password or other credentials from its clients

- Always use the latest web browsers versions.

Regards,

IT Security Team