

BEYOND THE PADLOCK

AVOIDING FRAUD ONLINE

Cybercrime will exceed \$2 trillion in 2019.¹

Phishing is a fraudulent attempt to obtain sensitive information, such as usernames, passwords and credit card details, by impersonating a trustworthy website.



482.5
million phishing
attacks in 2018 -
2x the attacks
in 2017²

Password: *****

Secure Sockets Layer (SSL) certificates encrypt the information sent between a device and server, or between two servers, to prevent cybercriminals from modifying data. There are three types of SSL certificates:



Domain Validation (DV): Certificate Authority (CA) confirms only that the registered domain is under the control of the certificate requestor.



Organization Validation (OV): Certificate Authority (CA) authenticates domain control AND authenticates the identity of the legal entity or individual that requested the certificate.



Extended Validation (EV): Certificate Authority (CA) follows a strict set of authentication procedures to ensure that the true identity of the certificate holder is represented.

 **SECURE** company-branded.com



99.99%
crime-free

**Sites with EV SSL
are nearly always
legitimate**

Georgia Tech Cyber Forensics Innovation Lab (CyFI) correlated sites with EV certificates to known criminal actors going back to 2010.

2.6 million
EV domains
analyzed

TOP TIPS to avoid falling victim to a malware attack or phishing scam when opening a link in an email or browsing on a computer.

1. Ensure website has a padlock symbol, indicating active SSL certificate.
2. Never input personal, credit card, or other sensitive data, when a "Not Secure" warning is present or there is no padlock symbol.
3. Look for company-branded address bars in popular browsers, indicating the highest level of validation.



 ralphlauren.com



 ETRADE Financial Corporation [US] |



 American Cancer Society, Inc. (US) |

The Georgia Tech CyFI Lab study "Understanding the Role of Extended Validation Certificates in Internet Abuse," was sponsored by Sectigo and published in July 2019. Sectigo (formerly Comodo CA) is the world's largest commercial Certificate Authority and a provider of purpose-built and automated PKI management solutions to secure websites, connected devices, applications, and digital identities. For more information, contact press@sectigo.com. [External Sources: (¹Juniper) (²Kaspersky Lab)]