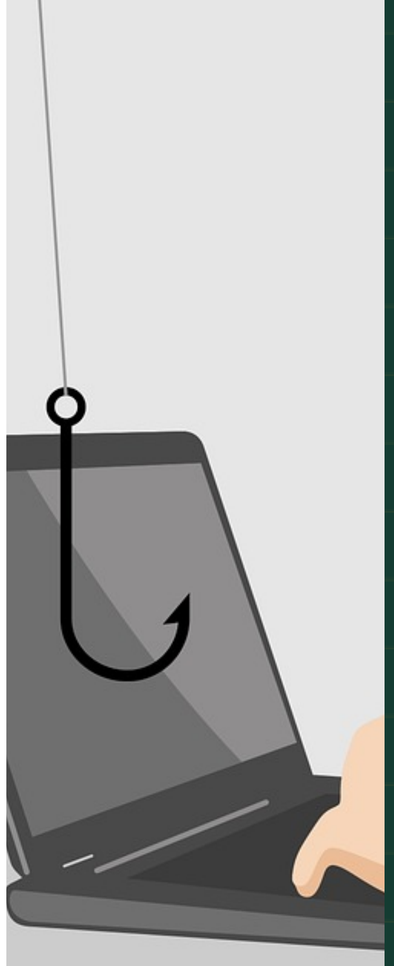
THE STATE OF E-COMMERCE PHISHING 2019

NormShield

As the holiday season ramps up, cybercriminals are launching new fraudulent e-commerce sites to trick consumers into handing over personal and financial information.
This report reveals our latest research on trends in website phishing, the probable impacts as a result of attacks and how to limit your risk.

E-commerce has so many benefits for both customers and businesses, including lower cost, time-saving, ease of use, and real-time transactions without geographical borders.

However, the coin always has two sides. The broad attack surface of e-commerce also gets the attention of hackers, especially during the peak shopping season.



E-Commerce Phishing at a Glance

50

NormShield investigated 50 major global e-commerce companies

6,000 +

Potential phishing domains registered so far in 2019 exceeds 6,000 and is expected to exceed 9,000.

11% increase

The number of potential phishing domains increased 11% compared to 2018.

3X

The number of potential phishing domains certified by registrars tripled in 2019 over 2018

E-Commerce Phishing Attacks

As the holiday season approaches, many e-shoppers are excited to buy gifts for their loved ones and take advantage of campaigns on Black Friday and Cyber Monday deals. Care also highly motivated by holiday shopping deals, although their motives are not in line with the spirit of holiday giving. They use fraudulent websites to not only mimick a genuine site, but also use in phishing emails that overpromise huge discounts, offer free gift cards, and make other enticing offers. The goal is to manipulate e-shoppers into entering personal information, credentials or credit card info that they can then use to make fraudulent purchases, steal identities or sell on the darknet.

2019

McAfee reported a phishing kit, called 16Shop, targeting Amazon customers

2017

Scammers took advantage of the popularity of online shopping during the holiday season

2016

Amazon Prime Day phishing email included invite to write a review on the product for $50 bonus credit

A security flaw found on eBay's website put millions of customers open to phishing

2015

Alibaba customers were victimized by a phishing attack with e-mails from feedback@ service.alibaba.com

2014

E-mail phishing scams pretended to be Walmart included gift card requiring activation

10,000 customers of Booking.com became victims of scammers using phishing email addresses

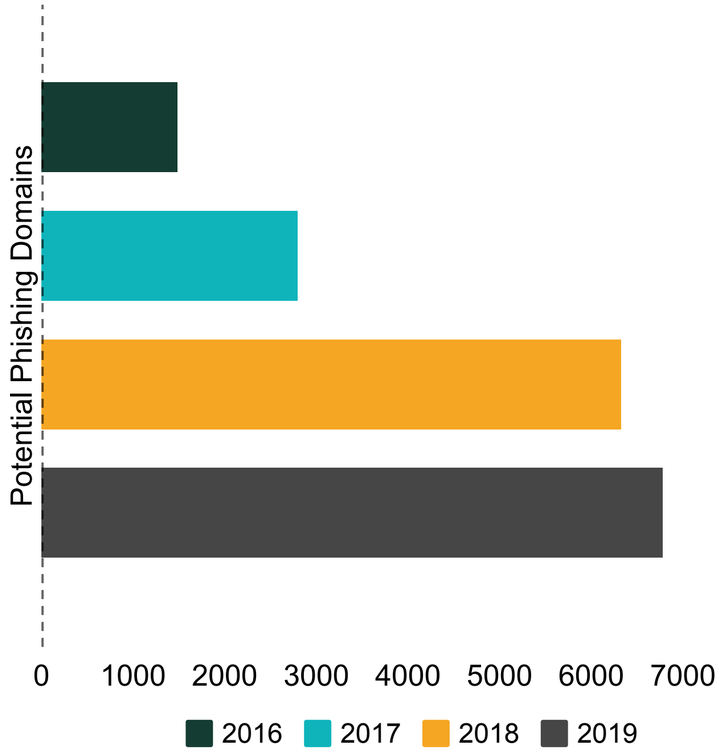
Phishing Domains are on the Rise

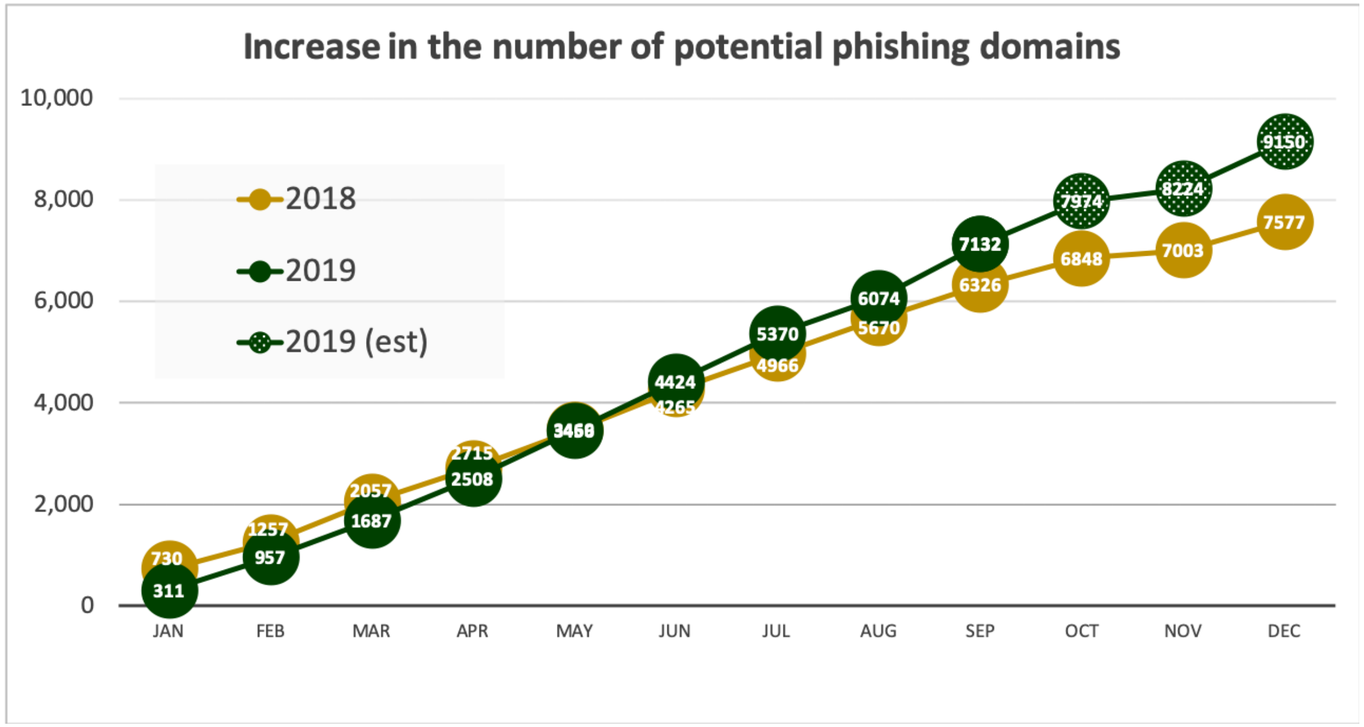
6X increase in the last four years

The number of potential phishing domains for 50 major e-commerce sites multiplied six times in the last four years. While under 1,000 in the first 9 months of 2016, it is more than 6,000 so far in 2019.

11% increase over 2018

The number of phishing domains registered in the first 9 months of 2019 is 11% higher than during the same period in 2018.





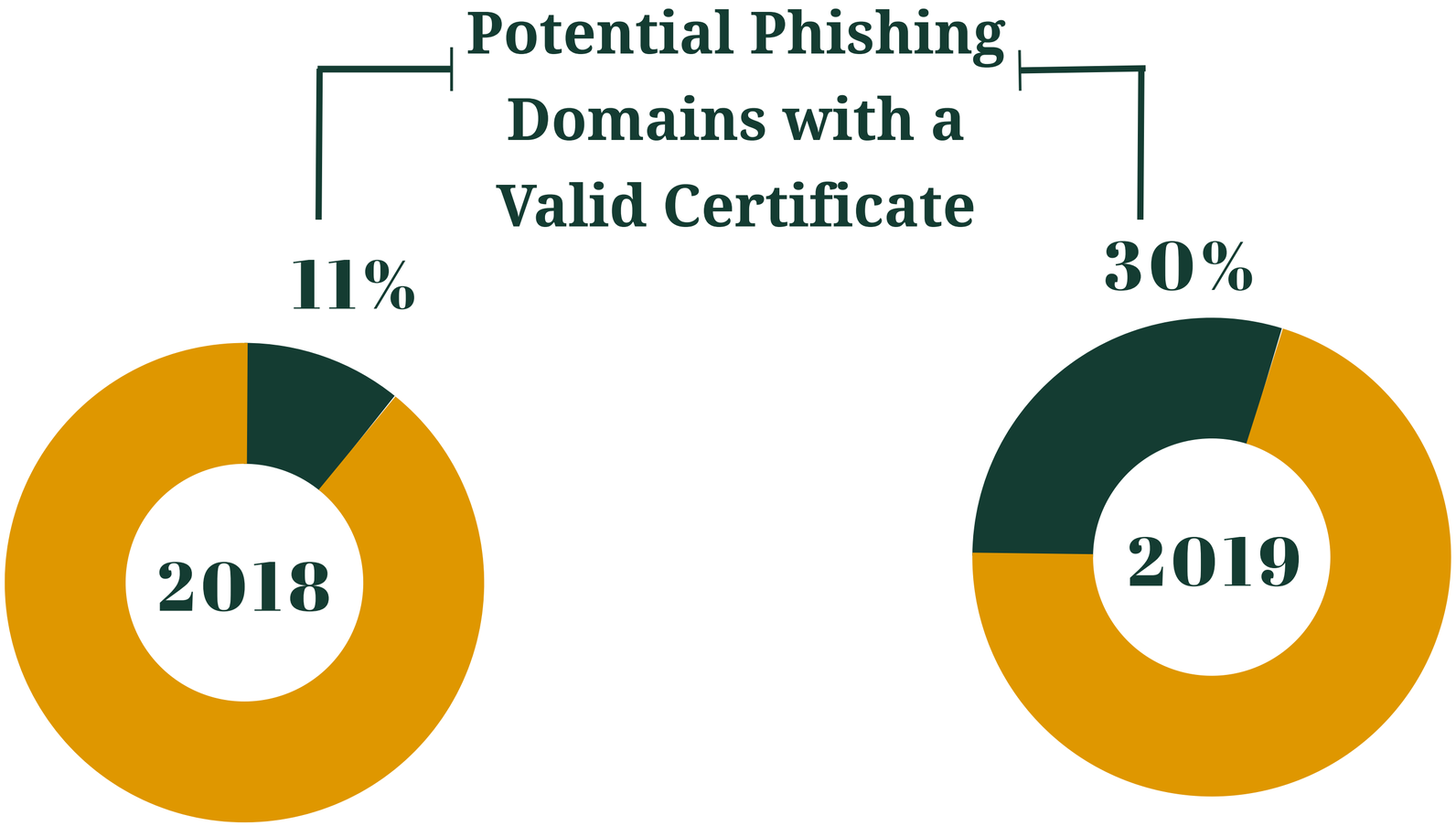
Expected to exceed 9,000

The projections, which take the holiday sea son into account, indicate that the number of potential phishing domains for 50 major e-commerce sites may exceed 9,000 by the end of the year.

Attacks in waiting

Hackers like to wait for the right moment. Some domains that were registered last year are still lying in wait and are at risk for activation at any time.

The Padlock Can Lie

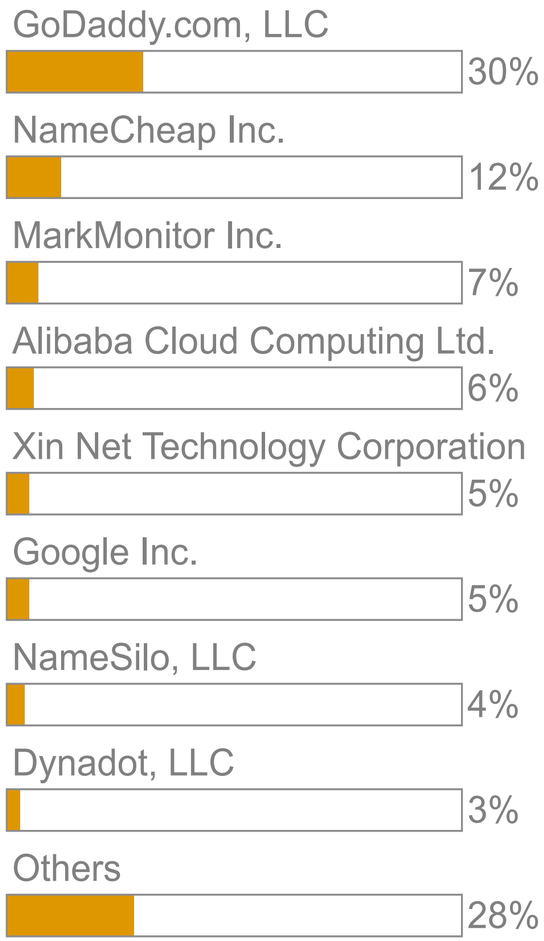


Hackers are creating more credible phishing websites every year. To gain higher levels of trust, they purchase legitimate certifications for fraudulent domains.

30% of the possible phishing domains registered in 2019 have certifications. When compared with 2018, the number of certified phishing domains are three times higher in 2019.

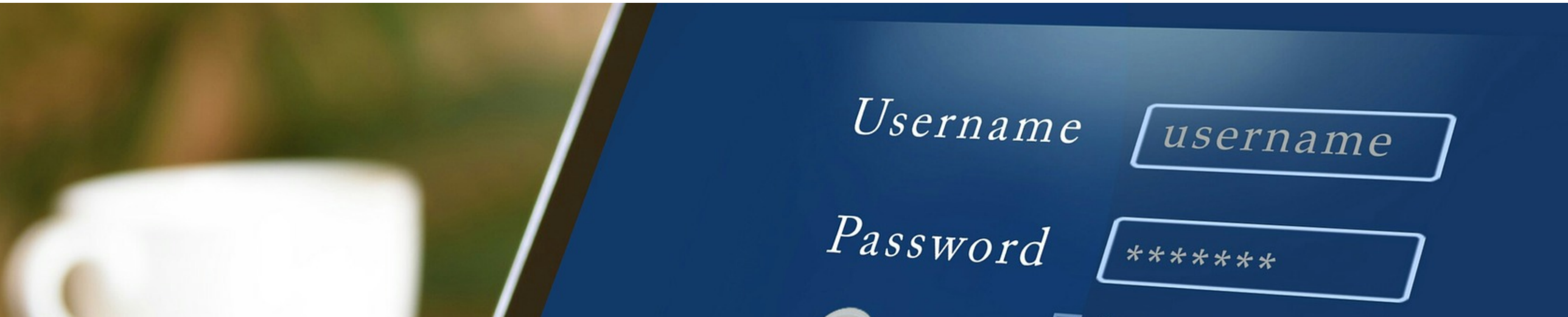
Every year, hackers become more resourceful and improve their techniques. So, the increase in the number of potential phishing domains with valid certificates poses more risks for e-commerce companies.

Top Registrars



Phishers use a wide variety of registrars to purchase domains. Registrars that offers free registration are often top choices.

E-commerce companies can use this information as another input to detect phishing sites.



Know the Risks

Supply Chain

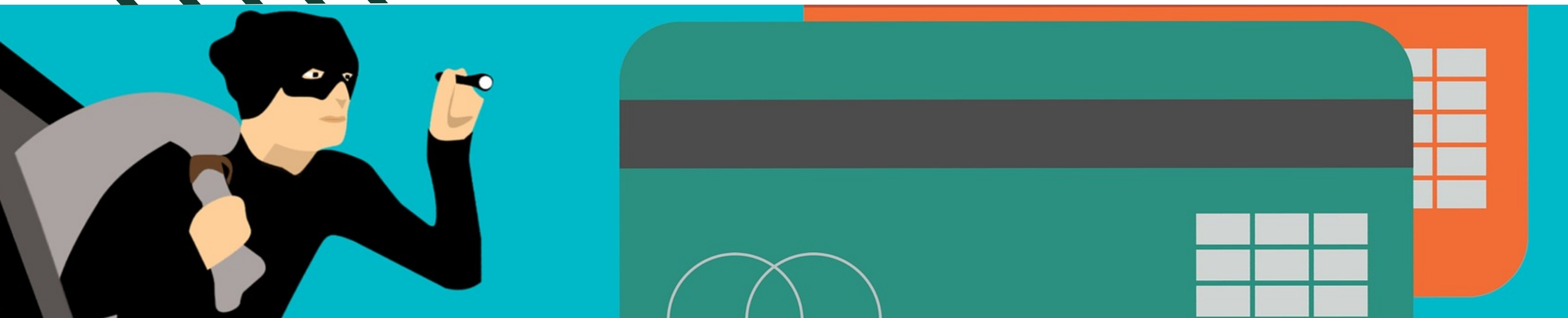
Brands and retailers often work with numerous e-commerce partners and affiliates who are trusted to sell their goods. Even if a brand's site has taken the proper security measures, how do they know if other selling their products are not susceptible to website phishing attacks? A phishing attack executed on a third-party can have a lasting impact.

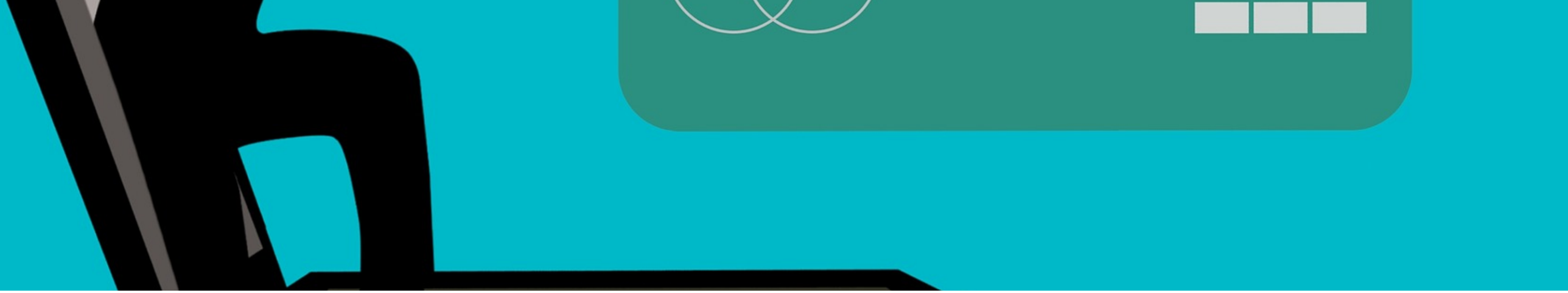
Digital Presence

Hackers don't always copy a complete website to execute phishing fraud. They also use social engineering, credential-based landing pages, or use individual brand images and elements to create fake deals while impersonating e-commerce sites like Amazon.

Customer Communication

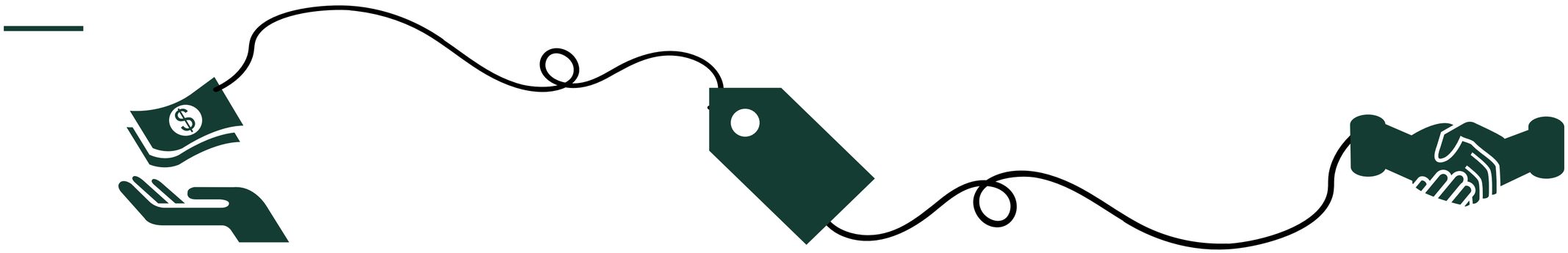
Consumers are primed to receive an overwhelming number of emails throughout the holiday season. Hackers are counting on consumers falling for their fake offers hidden in plain sight among real ones.





The global cost of online crime is expected to reach $6 trillion by 2021
– Cybersecurity Ventures

The Impact



Financial Impact

Website phishing has contributed to 1.3 billion in BEC losses in 2018.
(FBI internet crime report)

Brand Reputation

On average, more than 25% of a company's market value is directly attributable to its reputation.
(World Economic Forum)

Consumer Trust

One in every three consumers will no longer do business with a company if it suffers from a cyber-security breach.
(Deloitte)

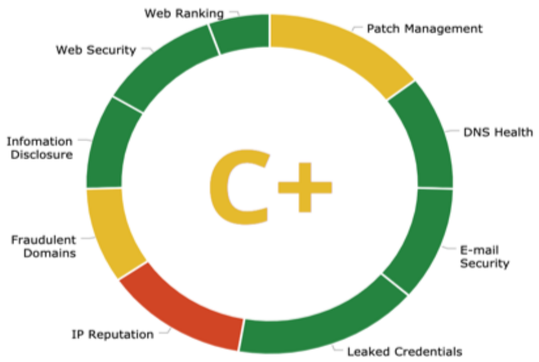
NormShield ®

Cyber Risk Monitoring

Trusted Security Rating Services

info@normshield.com

A Complete Cyber Risk Picture



Technical Cyber Risk Score
The NormShield cyber risk scorecards enable organizations to self-monitor their cyber risk posture and perform a non-intrusive 60 second cyber risk assessment of their suppliers. Executives get easy to understand scorecards with letter-grade scores and IT security teams can drill down to the technical details in each risk category.

Risk in Financial Terms
NormShield uses the FAIR model to calculate the financial impact (risk) to an organization if a cyber event would occur at a chosen supplier to cost-effectively achieve and maintain an acceptable level of loss exposure. FAIR has become the only international standard Value at Risk (VaR) model for cybersecurity and operational risk.

Questionnaire & Compliance Correlation
NormShield correlates findings to industry standards and best practices. The classification allows you to measure the compliance level of the target company for different regulations including **NIST 800-53, ISO27001, PCI-DSS, HIPAA, GDPR** and **Shared Assessments**.

Request a free scorecard