jscrambler

YOUR ONLINE SHOPPING FORM
IS A HACKER'S FAVORITE STORE

MAKE SURE YOUR FORMS ARE NOT LEAKING CUSTOMER DATA

1 WHAT YOU NEED TO KNOW

ONE IN THREE PEOPLE ARE ONLINE SHOPPERS

70% OF WEBSITE CLIENT-CODE COMES FROM **THIRD-PARTY SCRIPTS.**

2023 HAS **80 MILLION MORE DIGITAL BUYERS** THAN IN 2022.

75% OF ALL BREACHES VISA INVESTIGATED LAST YEAR INVOLVED E-COMMERCE SITES – WITH **DIGITAL SKIMMING ATTACKS AT THE TOP OF THE LIST**.

78% OF ONLINE SHOPPERS THINK **TWICE ABOUT BUYING FROM AN ONLINE** RETAILER AFTER A BREACH.

TIP

MONITORING SCRIPTS FOR MALICIOUS BEHAVIOR AND ASSESSING THE RISK OF FORMS LEAKING DATA ON YOUR CHECKOUT PAGED MUST AT THE TOP OF YOUR LIST!

2 MORE ONLINE SALES, MORE SECURITY RISKS

IF YOU ACCEPT ONLINE PAYMENTS, **YOU ARE A TARGET** FOR E-SKIMMING ATTACKERS.

IF YOU HAVE THIRD-PARTY SCRIPTS AND ADD-ONS POWERING YOUR WEBSITE, **YOU HAVE MULTIPLE GATEWAYS FOR WEB SKIMMERS.**

IF YOU THINK HAVING THIRD-PARTY PAYMENT PROCESSORS MAKES YOUR CHECKOUT SAFE, (WELL) **THINK AGAIN.**

IF YOUR WEBSITE INCLUDES PAYMENT FORMS, **TAKE THE STEPS TO MITIGATE THE RISK OF DATA COMPROMISE**

TIP

AT JSCRAMBLER, WE RECOMMEND E-COMMERCE SITES AND ONLINE RETAILERS FREQUENTLY AUDIT THEIR WEB STOREFRONT CODE FOR MALICIOUS BEHAVIOR AND ENSURE THEIR SUPPLIERS FOLLOW THE SAME CLIENT-SIDE SECURITY PRACTICES.

BE SURE YOUR CHECKOUT PAGES ARE NOT LEAKING DATA.
AVOID BECOMING ONE OF THE FOLLOWING EXAMPLES:

300K

IN MAY AND JUNE 2023, AN UNAUTHORIZED THIRD PARTY INSERTED MULTIPLE INSTANCES OF MALICIOUS CODE INTO SEVERAL E-COMMERCE CHECKOUT PAGES.

ATTACKERS STOLE THE PAYMENT CARD DATA OF MORE THAN 300,000 INDIVIDUALS.
*SOURCE: SECURITYWEEK (2023)

60M

ALMOST 60 MILLION COMPROMISED PAYMENT CARD RECORDS HAVE BEEN FOR SALE ON DARK WEB PLATFORMS IN 2022.

DIGITAL SKIMMING ACTORS LAUNCHED CAMPAIGNS THAT EMPLOYED FAKE PAYMENT CARD FORMS.
*SOURCE: RECORDEDFUTURE (2022)

70K

AS OF 2022, MORE THAN 70,000 STORES ARE ESTIMATED TO HAVE BEEN COMPROMISED WITH A WEB SKIMMER.
*SOURCE: THEHACKERNEWS (2023)

$20M

ONCE A DATA BREACH IS REPORTED, BUSINESSES MAY FACE FINES OF UP TO €20 MILLION OR 4% OF THEIR GLOBAL REVENUE FROM THE PREVIOUS YEAR, ACCORDING TO GDPR.
*SOURCE: GDPR (DATE: N/A)

3 ASSESS THE RISK OF WEBSITE FORMS AND CHECKOUT PAGES LEAKING DATA WITH FIVE QUESTIONS

DO YOU HAVE AN INVENTORY OF ALL JAVASCRIPT RUNNING ON YOUR CHECKOUT PAGES?

DO YOU KNOW **WHO REQUESTED EACH SCRIPT AND FOR WHAT REASON**?

ARE YOU EXPOSED TO E-COMMERCE **SKIMMING ATTACKS?**

ARE YOU MONITORING SCRIPTS FOR SIGNS OF **INFECTION OR MISBEHAVIOR?**

ARE DIGITAL PARTNERS ACCESSING YOUR **USERS' PAYMENT DATA WITHOUT AUTHORIZATION**?

TIP

CHECK THE THIRD-PARTY CODE RUNNING ON YOUR WEBSITE. VERIFY IF IT IS BEHAVING AS IT SHOULD.

4 AUTOMATE CLIENT-SIDE PROTECTION WITH JSCRAMBLER

BENEFIT 1: MAINTAIN AN INVENTORY OF ALL PAYMENT SCRIPTS WITH BUSINESS JUSTIFICATION

BENEFIT 2: ENSURE ONLY APPROVED SCRIPTS ARE RUNNING ON PAYMENT PAGES

BENEFIT 3: PREVENT ATTEMPTS TO COMPROMISE USER PAYMENT DATA.

BENEFIT 4: MITIGATE THE RISK OF ATTACKS AND MALICIOUS CODE INJECTIONS

BENEFIT 5: MONITOR, ALERT, AND BLOCK ALL MALICIOUS BEHAVIORS

BENEFIT 6: COMPLY WITH NEW PCI DSS V4.0 PAYMENT PAGE REQUIREMENTS

TIP

START PLANNING TODAY TO COMPLY WITH PCI DSS V4.0 AND THE NEW PAYMENT PAGE JAVASCRIPT REQUIREMENTS

COMPLY WITH PCI DSS V4.0 PAYMENT PAGE REQUIREMENTS 6.4.3. AND 11.6.1.

JSCRAMBLER IS PURPOSE-BUILT TO OVERCOME THE DYNAMIC AND INSECURE NATURE OF PAYMENT PAGES THROUGH AUTOMATED CLIENT-SIDE RISK VISIBILITY, CONTROL AND COMPLIANCE.

ENSURE A TRUSTED AND SECURE EXPERIENCE FOR YOUR ONLINE CUSTOMERS THROUGH THE HOLIDAY SEASON

KNOW YOUR FORMS

WWW.JSCRAMBLER.COM