ENJOY SAFER TECHNOLOGY™

SMALL BUSINESS CYBERSECURITY: A QUICK PRIMER

An educational eye-opener for small businesses.

THE PROBLEM? STAFFING AND BUDGET SHORTFALLS.

69% don't have sufficient security budget, in-house expertise or both [1]

1 in 5 have no security at all [2]

EXPERIENCE: NOT THE BEST TEACHER

61% of all data breach victims are businesses with **under 1,000** employees [3]

HALF of SMBs have experienced breaches of customer and employee information [1]

THE RISING COST OF A LESSON LEARNED

Cost of breaches per business: [1]

PASSWORDS: NOT PASSING THE TEST

63% of all data breaches involve weak, default or stolen passwords [4]

3 in 5 SMBs do not have visibility into employees' password practices [1]

TWO-FACTOR AUTHENTICATION: THE SMARTER CHOICE

65% of point-of-sale system breaches use stolen passwords [3]

PCI DSS now requires multi-factor authentication for administering systems that access card data

THE ABCs OF SMALL BUSINESS CYBERSECURITY

Assess assets, risks & resources
Know what you need to protect

Build your security policy
Spell out what's allowed and what isn't

Choose your security controls
Identify practices and technologies to enforce policies

Deploy your controls
Test to ensure controls work for the business

Educate staff, execs & vendors
Raise awareness and reinforce policies

Further assess, audit & test
Update as threats evolve and business changes

www.eset.com

1 2016 State of Cybersecurity in Small & Medium-Sized Businesses (SMB), Ponemon Institute
2 Small Business Cybersecurity Survey Conducted by Google Consumer Surveys, April 2016
3 2017 Verizon Data Breach Investigations Report
4 2016 Verizon Data Breach Investigations Report