WEBROOT®
Smarter Cybersecurity™

WHY YOU NEED SECURITY AWARENESS TRAINING

You might not think you need to educate end users about cyberattacks, compliance issues, and other risks they face online.

"My business is too small to be a target."

"I don't handle healthcare records, so I don't have compliance regulations."

"My end users would never click a phishing link."

There are lots of excuses.
But here's the thing...

Every business is a target.

And there's a reason regulated industries like healthcare, finance, energy, and others require Security Awareness Training for end users.

LET'S LOOK AT SOME REAL-WORLD SCENARIOS.

(WE'VE REMOVED BUSINESS NAMES TO PROTECT THEIR REPUTATIONS.)

REAL-WORLD SCENARIOS

FASHION HOUSE GETS PHISHED

Company Profile

» Privately held women's apparel co.
» $4 – 5 million annual revenue
» 20 – 25 employees

An administrative assistant received an email from the CEO, who was on vacation at the time. The email had instructions to wire $500,000 to a vendor, and included the account details. The assistant immediately contacted the finance team, who made the transfer at once.

The email was not from the CEO, and neither the assistant nor the Finance team verified any of the information before making the transfer. When the CEO returned, they contacted the FBI at once, but the funds were never recovered.

Loss: $500,000

MAJOR HEADACHES FOR HEALTH CLINIC

Company Profile

» 40+ year-old neurology clinic
» $75 million annual revenue
» 40 – 45 employees

While investigating a ransomware attack, the clinic's IT team discovered a separate data breach, in which an attacker had access to patient records—including names, Social Security numbers, driver's license, addresses, phone numbers, medical data, prescriptions, and insurance data—for 15 months.

Up to 400K patient records may have been compromised. The average healthcare data breach cost $380 per record[1] in 2017. Let's do the math.

Loss: Up to $152 Million

THE HIGH COST OF A FAKE INVOICE

Company Profile

» Food distributor
» $20 million annual revenue
» 20 – 25 employees

The company got an invoice email that looked to be from a trusted vendor. While it contained new wire transfer details, the email looked legitimate. It also arrived around the same time the vendor usually sent invoices, and was for an expected amount, indicating the thieves had been watching the company's dealings for some time.

The company didn't discover the problem until the real vendor got in touch to ask why the payment was late. By then, nothing could be done.

Loss: $23,500

SCHOOL DISTRICT SCAMMED

Company Profile

» School district
» Over 2,100 employees, including 630 teachers

An attacker spoofed the district superintendent's email address, requesting personal information of the district's staff members. Over 2,000 employee records, including names, addresses, salaries, and Social Security numbers were compromised in the breach. Although the district notified the affected employees and the proper authorities immediately, the damage was done.

According to the Ponemon Institute, the average cost of a data breach in the education sector in 2017[1] was $200.

Loss: Up to $400,000

[1]Ponemon Institute. "2017 Ponemon Cost of Data Breach." (June 2017)

WHERE DOES SECURITY AWARENESS TRAINING FOR END USERS FIT IN?

Think about the four scenarios above. 3/4 of those situations started with a fake email. The last one involved a ransomware attack and a long-term data breach. Since phishing emails are responsible for 73% of malware and ransomware[2] attacks, it's likely a fake email was involved somewhere in the early stages of that scenario too.

If the end users at those companies were better trained at spotting fake emails, they would have saved a lot of time, headache, and money.

Now think about the other bad habits most people have online. Reusing passwords and storing confidential data improperly are other common examples.

90% of successful network breaches are caused by user error.

80% of hacking-related breaches[3] leverage either stolen and/or weak passwords.

94% of phishing attacks[3] that lead to a breach are followed by some sort of software installation.

15% of users who fall for a phishing attack once[3] will take the bait a second time.

66% of malware[3] is installed via malicious email attachments.

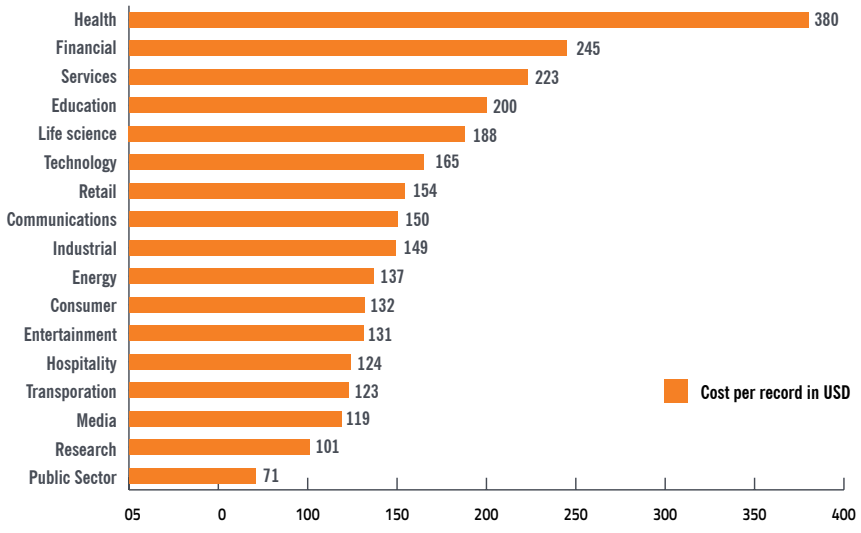
STILL NOT CONVINCED? LET'S SEE WHAT YOUR COSTS MIGHT BE.

Think about the four scenarios above. 3/4 of those situations started with a fake email. The last one involved a ransomware attack and a long-term data breach. Since phishing emails are responsible for 73% of malware and ransomware attacks, it's likely a fake email was involved somewhere in the early stages of that scenario too.

If the end users at those companies were better trained at spotting fake emails, they would have saved a lot of time, headache, and money.

Now think about the other bad habits most people have online. Reusing passwords and storing confidential data improperly are other common examples.

Cost of a data breach per record lost, by industry[1]



[2] NTT. "Global Threat Intelligence Report 2017." (April 2017)
[3] Verizon. "2017 Data Breach Investigations Report." (April 2017)

HERE'S A QUICK CHECKLIST

Do you work in any of the following industries?

Finance

Healthcare / Pharmaceutical

Retail

Insurance

Energy / Utilities

Do you take credit card payments or wire transfers for any reason?

Do you store customers' personal data (SSNs, account numbers, payment card data, etc.) for any length of time?

IF YOU ANSWERED YES TO ANY OF THE ABOVE,

then you are subject to mandatory compliance and/or cybersecurity regulations.

(and the hefty fines that come from non-compliance.)

SO WHAT CAN YOU DO?

1

Don't publicize executives' email addresses.
Criminals use that information.

2

Don't publicize your organizational structure.
Criminals use that for social engineering, too.

3

Enforce 2-factor authentication across your business.
That includes vendor information changes, etc.

4

Pick up the phone.
If an email looks phishy, call the sender personally using their official phone number, not a number listed in the email, and add phone verification to your payment/wire transfer process.

5

Train your users.
We all know "common sense" isn't as common as we hope. Train end users how to use good judgement and report anything out of the ordinary to IT and security teams.

6

Perform regular security audits and phishing simulations.
This gives you real-world insight into end users' behavior, and the problem areas you need to address.

FOR MORE INFORMATION ON HOW TO EDUCATE USERS AND KEEP YOUR BUSINESS SAFE, VISIT WEBROOT.COM/AWARENESS