SOLUTION BUILDERS®

CYBERSECURITY AWARENESS MONTH 2026

THE CYBERSECURITY APOCALYPSE

A survival field guide to the **7 monsters** hunting your business.



Real threats. Real data.
Slightly ridiculous costumes.

SWIPE TO MEET THEM →

KNOW WHAT IS OUT THERE

Seven monsters. All of them real.

Every creature in this guide is a threat showing up in this year's breach data. The costumes are the only part we made up.



COUNT PHISHULA

Real name: **Phishing**

THREAT LEVEL

62%



THE RANSOM MUMMY

Real name: **Ransomware**

THREAT LEVEL

48%



THE BOTNET HORDE

Real name: **Botnets**

THREAT LEVEL

97%



THE VENDOR WEREWOLF

Real name: **Third party risk**

THREAT LEVEL

48%



THE FRANKEN SYSTEM

Real name: **Unpatched technology**

THREAT LEVEL

31%



THE DEEPFAKE SHAPESHIFTER

Real name: **AI impersonation**

THREAT LEVEL

45%



THE SHADOW AI GHOST

Real name: **Shadow AI**

THREAT LEVEL

43%

Each number is explained, with its source, on the monster's own page.



MONSTER 01

COUNT PHISHULA

REAL NAME · PHISHING

Charming, well dressed, and completely unable to enter unless somebody invites him in. One click is an invitation.

THREAT LEVEL

HOW IT HUNTS

Arrives dressed as your bank, your boss, or a delivery notice. Asks very nicely for a password, a payment, or a quick favor.

Phishing was the most reported cybercrime in America last year, with 191,561 complaints to the FBI.

THE SCARY NUMBER

62%

of breaches involve a person clicking, replying, or trusting the wrong message

HOW TO SURVIVE

- Hover over every link before you click it
- Confirm any money request with a phone call
- Train the team until spotting bait is a reflex

Source: Verizon Data Breach Investigations Report 2026. FBI Internet Crime Report 2025.



MONSTER 02

THE RANSOM MUMMY

REAL NAME · RANSOMWARE

Wraps every file you own in layers you cannot undo, then demands tribute to unwrap them.

THREAT LEVEL

HOW IT HUNTS

Slips in through a phish or an unpatched system, waits quietly, then locks everything at once. Usually on a weekend.

The median ransom paid was $139,875. The good news is that 69% of victims refused to pay.

THE SCARY NUMBER

48%

of all breaches now involve ransomware, up from 44% a year ago

HOW TO SURVIVE

- Keep tested backups: three copies, two media types, one off site
- Put 24/7 detection and response on every device
- Write the plan for the bad day before the bad day

Source: Verizon Data Breach Investigations Report 2026.



MONSTER 03

THE BOTNET HORDE

REAL NAME · BOTNETS

Thousands of hijacked computers, cameras, and routers shuffling wherever their master points. Yours could be one of them.

THREAT LEVEL

HOW IT HUNTS

Guesses passwords by the million, floods websites until they fall over, and infects whatever it touches next.

A zombie device usually works fine. That is the scary part. Nobody notices it joined the horde.

THE SCARY NUMBER

97%

of identity attacks are password guessing at massive scale, the horde's favorite snack

HOW TO SURVIVE

- Turn on MFA for every account, no exceptions
- Update routers, cameras, and anything else with a plug
- Watch your network for traffic that should not be there

Source: Microsoft Digital Defense Report 2025.



MONSTER 04

THE VENDOR WEREWOLF

REAL NAME · THIRD PARTY RISK

Looks exactly like a vendor you have trusted for years. Then the moon comes up.

THREAT LEVEL

HOW IT HUNTS

Attackers breach one of your suppliers, then stroll into your network with their keys. No forced door, no alarm.

You can have great security and still get bitten through a partner who does not.

THE SCARY NUMBER

48%

of breaches involved a third party, a 60% jump from the year before

HOW TO SURVIVE

- Give vendors only the access they truly need
- Ask partners how they protect themselves, and get proof
- Monitor vendor accounts as closely as your own

Source: Verizon Data Breach Investigations Report 2026.



MONSTER 05

THE FRANKEN SYSTEM

REAL NAME · UNPATCHED TECHNOLOGY

Stitched together from old servers, forgotten laptops, and software that stopped getting updates years ago. It is alive. Barely.

THREAT LEVEL

HOW IT HUNTS

Every missing patch is an open seam. Attackers do not need to be clever. They just pull the thread.

Only 26% of critical known flaws were fully patched last year, and the typical fix took 43 days.

THE SCARY NUMBER

31%

of breaches begin with an attacker exploiting a known, unpatched flaw

HOW TO SURVIVE

- Patch on a schedule, not when somebody remembers
- Retire anything the manufacturer no longer supports
- Keep an inventory. You cannot protect what you forgot you own

Source: Verizon Data Breach Investigations Report 2026.



MONSTER 06

THE DEEPFAKE SHAPESHIFTER

REAL NAME · AI IMPERSONATION

Wears your CEO's face and borrows your CFO's voice. It sounds like someone you trust because it studied them.

THREAT LEVEL

HOW IT HUNTS

A video call or a voicemail with an urgent request: wire the money, share the code, and keep it quiet.

More than one in four organizations hit by an attack say AI was part of it, up 56% in a year.

THE SCARY NUMBER

45%

of AI powered attacks use deepfake impersonation of someone the victim trusts

HOW TO SURVIVE

- Agree on a safe word for money and password requests
- Call back on a number you already have on file
- Slow down. Urgency is part of the costume

Source: IBM Cost of a Data Breach Report 2026.



MONSTER 07

THE SHADOW AI GHOST

REAL NAME · SHADOW AI

Friendly, helpful, and already inside the building. It is the AI tool nobody approved, quietly reading whatever gets pasted into it.

THREAT LEVEL

HOW IT HUNTS

It does not attack at all. It floats through the walls with your client data, contracts, and source code.

These incidents cost more too: $5.39 million on average, compared with $4.63 million.

THE SCARY NUMBER

43%

of organizations had a shadow AI incident this year, up from 20%

HOW TO SURVIVE

- Write a simple AI policy people will actually read
- Give the team approved tools so they stop hunting for their own
- Know which data is going where, and who sent it

Source: IBM Cost of a Data Breach Report 2026.

PACK BEFORE NIGHTFALL

Your apocalypse survival kit.

No silver bullets, garlic, or torches required. Eight boring, proven habits beat all seven monsters.

MFA on every account

Repels: The Botnet Horde



Regular phishing training

Repels: Count Phishula



Tested, off site backups

Repels: The Ransom Mummy



A call back rule for money

Repels: The Deepfake Shapeshifter



A simple AI use policy

Repels: The Shadow AI Ghost



Tight limits on vendor access

Repels: The Vendor Werewolf



A real patching schedule

Repels: The Franken System



24/7 monitoring and response

Repels: All of them, all night

The honest truth: none of this is exotic. The businesses that get eaten are usually missing two or three of these basics.

ONE LAST SURVIVAL TIP

Nobody survives the apocalypse alone.

Solution Builders has been keeping businesses safe since 1995, with a 24/7 security team that does not scare easily.

30+
years in business

Top 1%
of MSPs nationwide

24/7
security operations



www.solutionbuilders.com
(952) 854 8188 · Book a free discovery session

Talk to a security architect →