



The Connected Contractor

AI, Automation, and Cybersecurity You Can Actually Use

Presented by Kevin Fox | President, FoxWerx Group

Today's Roadmap

01

AI You Can Actually Use

03

How It All Connects

05

Spot the Scam (Interactive)

07

Q&A + Bonus Tools

02

Live AI Receptionist Demo

04

Cybersecurity 101 for Contractors

06

Simple Steps to Stay Safe



BONUS TOOLS + FREE ACCESS

You get free access to:



WonderWerx Group on Skool

(tools, trainings, checklists)



AI Essentials Course



Cyber Safety Checklist

→ Scan the QR code on the next slide



WONDERWERX



Comment, "I met you at MICA"

What Is AI Really?

It's not The Terminator.

It's advanced software that can *think a little* and *act fast*.

It learns from patterns — and then *helps* with decisions or tasks.

Think:

- Call handling
- Email replies
- Scheduling
- Reviewing data
- Spotting risk



Why AI Matters to MICA

1 Industry Challenge

Increasing competition, rising customer expectations

2 Opportunity

AI tools provide competitive advantage without massive investment

3 Reality Check

35% of construction companies and contractors have already adopted some form of AI technology

Source: ConstructConnect Annual Technology Adoption Survey (2024)



So, how can you integrate
AI into your business today?

Getting Started With AI

AI Voice Receptionist

Handles missed calls, books jobs

AI Web Chat

Engages site visitors, collects leads 24/7

AI SEO Expert

Optimizes your site, helps you rank locally

AI Reputation Manager

Monitors reviews, flags issues

AI Sales Assistant

Sends follow-ups automatically

Each one saves time, captures leads, and helps you grow.

Real-World Case Study – AI in Action

The Problem

One of my clients was losing 40% of leads because he was too busy to answer calls.

The Solution

We set him up with an AI receptionist.

The Result

In 3 months, his booked jobs increased by 30%.

The ROI

The average ROI for AI receptionist technology was reported at 286% within the first year.

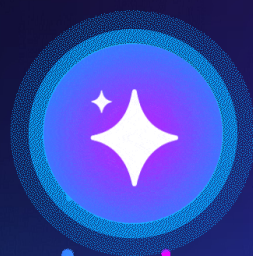
"Every business is writing its own story. Some are growing, evolving, adapting. Others are standing still, waiting for things to go back to the way they were. But business doesn't work that way. Progress doesn't wait."

"So here's the real question: What happens next?"





HOW DO YOU FIX IT?



INTRODUCING, YOUR
AI FRONT DESK

AI FRONT DESK

Your new 24/7 AI employees that cost less than a daily coffee run.



Answers every call

No matter when - even at 8pm on Saturday



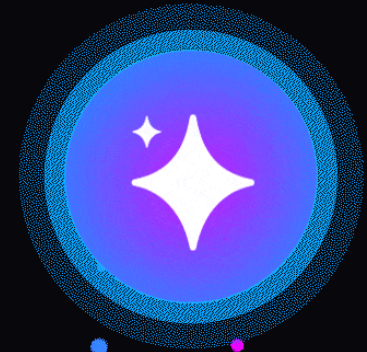
Captures contact info

No matter what - complete data collection



Feeds your CRM

No manual entry - instant
data integration



THE 90-DAY TRANSFORMATION

Here's what happened when we implemented this with a builder in Texas:

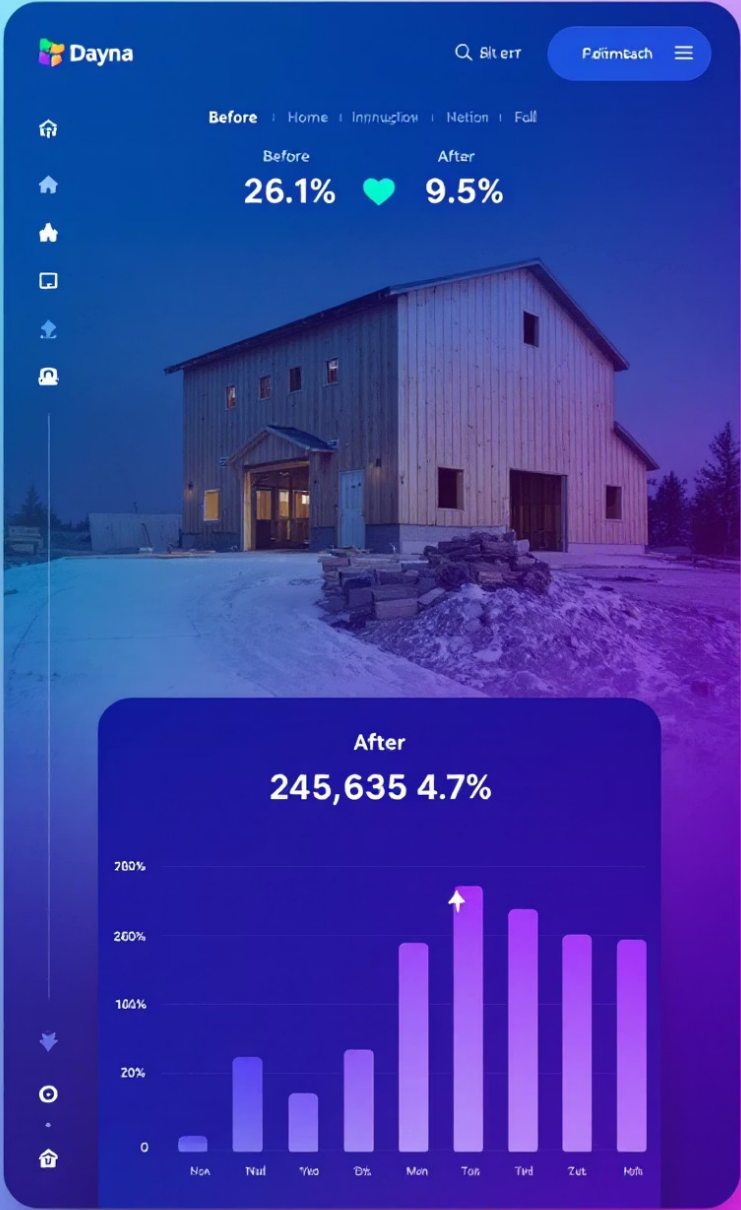
68% increase in conversions

44% increase in revenue

Metric	Before	After
Lead Contact Rate	58%	100% within 5 minutes
Close Rate	22%	37%
Quarterly Revenue	\$212K	\$306K

Capture 100% of opportunities and convert nearly twice as many into paying customers.

Same ad spend. Same team. **44% more revenue.**



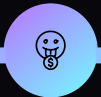
THE THREE-PART PROFIT EQUATION

Most businesses focus on the wrong part of the equation:



Lead Generation

What everyone obsesses over



Lead Conversion

Where the money is made



Client Fulfillment

Where your reputation is built

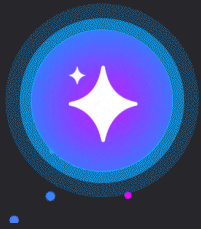
Here's the truth: Increasing your conversion rate by 10% is cheaper and faster than increasing lead volume by 10%.



WHAT DOES THIS
LOOK LIKE?

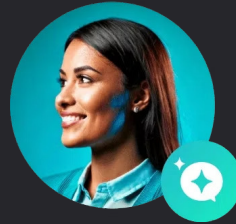


Your AI Front Desk



AI Chat Receptionist

Engages website visitors instantly. Answers questions and qualifies leads while you focus on building.



AI Voice Receptionist

Answers calls 24/7, routing inquiries with human-like conversation. Never misses an opportunity.



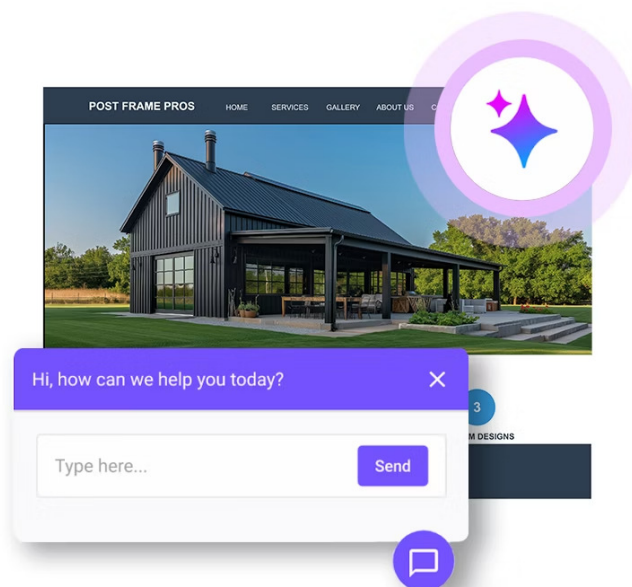
AI Review Specialist

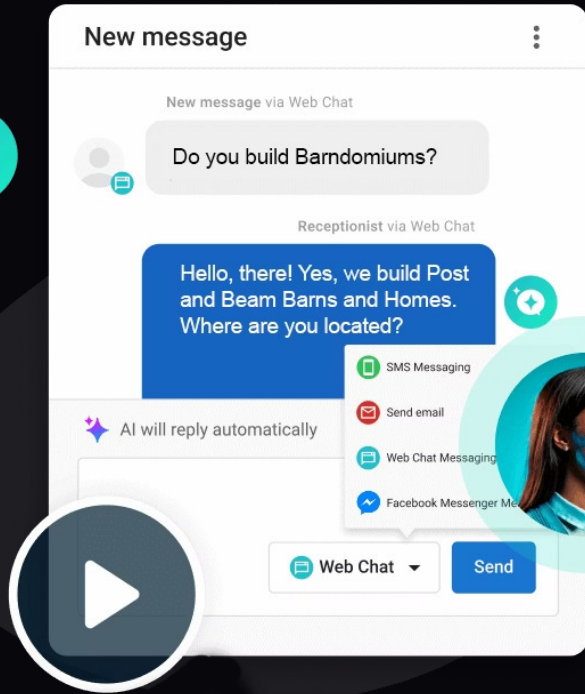
Monitors and responds to customer feedback. Builds your reputation while you build structures.

Your digital workforce works in harmony, handling crucial business tasks around the clock. Each AI assistant specializes in different aspects of your customer journey, creating a seamless experience. All anchored by an integrated CRM.



Increase **lead capture**
and **conversion** with
AI Web Receptionist.

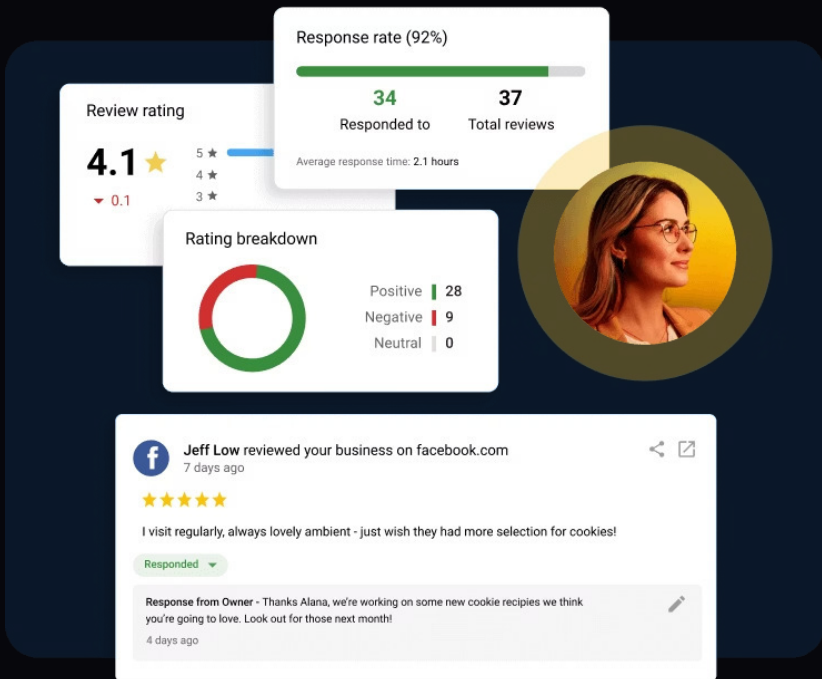




Receptionist

Never Leave A Lead Waiting

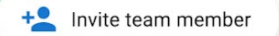
Provides fast, helpful responses through **phone, chat, text, or connected sites**. Answers questions, promotes services, books appointments, and handles support issues.



Reputation Specialist

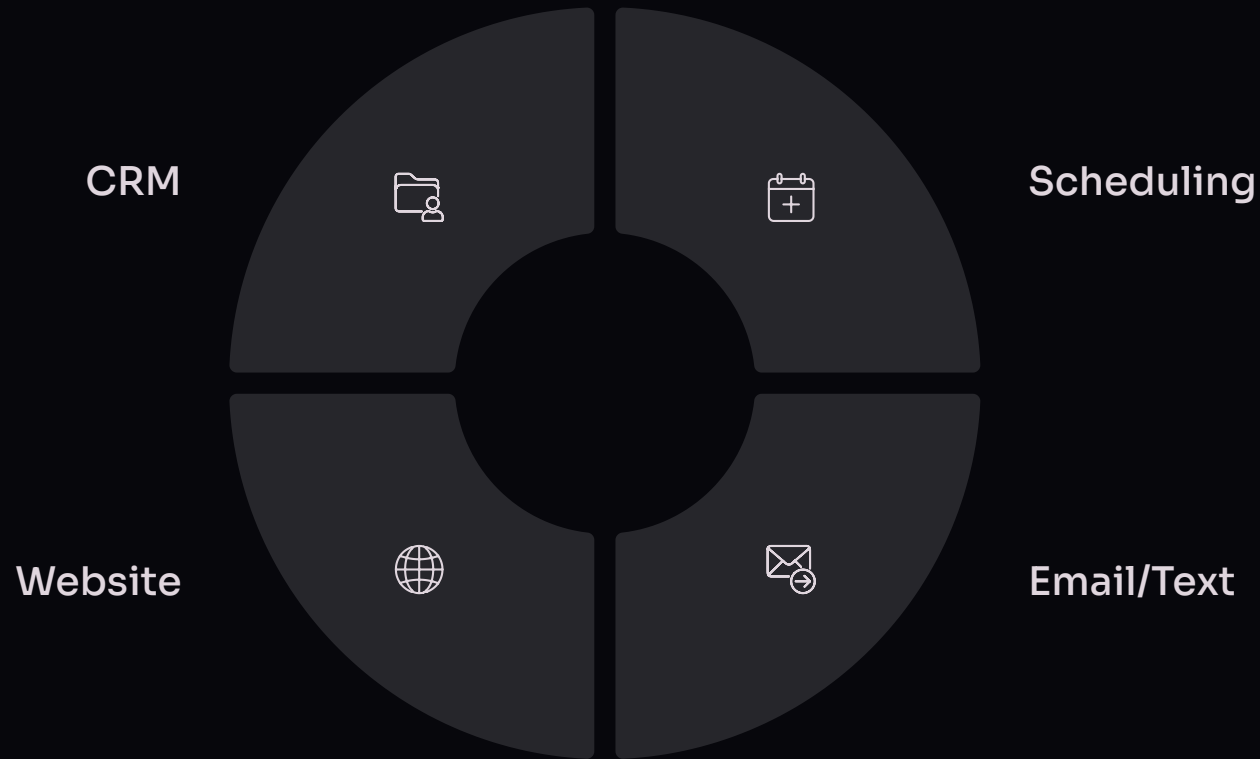
Cultivate a strong online reputation

Crafts thoughtful responses to reviews, posts on behalf of the business, and generates review requests to get more positive feedback and handle negative ones.



The Hidden Benefit: Data + Smart Systems

AI works best when connected to your:



Together, it becomes a **business system** — not just a bunch of disconnected tools.

"Think of it like a team of assistants who share the same brain."



Next Up...Cybersecurity 101



AI+Cybersecurity

Presented by Kevin Fox | FoxWerx Group

Today's Roadmap

01

Cybersecurity 101 for Contractors

03

Simple Steps to Stay Safe

02

Spot the Scam (Interactive)

04

Q&A + Bonus Tools



AI Isn't Just Smart, It's Safe

AI also strengthens your business by protecting it:

- Blocks phishing emails
- Detects strange logins
- Warns about weak passwords
- Learns from cyberattacks
- Powers training tools

"AI isn't just your new assistant—it's your silent security guard."

AI for Cybersecurity

AI can help *automate protection*:

- Spam and phishing filtering
- Fraud detection (bank logins, IP monitoring)
- Smart alerts
- Policy enforcement

It can even train your team:

"Is this email safe?" Let an AI assistant guide them through why or why not.

The #1 Cybersecurity Threat for SMBs

The Phishing Chain: From Click to Catastrophe

Phishing isn't just about a single malicious email; it's often the first step in a cascade of severe cyberattacks. Understanding this chain reaction is crucial for effective defense.



Initial Phishing Attack

The bait: a deceptive email or message designed to trick users.



Data Breaches & Theft

Once access is gained, sensitive information can be stolen or compromised.



Ransomware & Extortion

Systems are locked down, demanding payment for their release, or data is threatened to be leaked.



Financial Fraud

Attackers initiate fraudulent transactions, wire transfers, or manipulate invoices.



Business Disruption & Damage

Operations halt, reputation suffers, and recovery costs can be substantial.



E-BOOK

21 DIGITAL LIES

HACKERS WANT YOU TO BELIEVE

Get your Free E-Book and other resources
in the WonderWerx Community



WONDERWERX



Comment, "I met you at MICA"

What can YOU do? Cybersecurity 101

Why it matters:

- You handle customer data, bids, jobsite info
- You're a target — not an afterthought
- Ransomware hits small business just as often as big ones

One phishing link can:

- Lock your files
- Drain your bank account
- Spoil your reputation

Keep Your Eyes Peeled



Weird email address



Sense of urgency



Odd links



Misspelled domains



Generic greeting

Spotting Phishing Emails: 10 Real Examples & Red Flags

What is phishing? — fraudulent emails using social engineering to trick users into revealing sensitive info



Phishing Defined & Typical Tactics

What is Phishing?

Phishing = deceptive messages (often email) that try to get you to click links/download attachments or give personal info (passwords, SSNs, etc.)

Uses social engineering — exploiting trust, urgency, fear

Common Tactics Include:

- Urgency / threats (account being closed, suspension)
- Impersonating trusted services (banks, social media, Apple, IRS)
- Generic greetings, grammar mistakes, suspicious sender addresses

Phishing Email Example Types (Part 1)

1

Social Media Phishing

- Email pretending to be from LinkedIn, Facebook, etc.
- Urges password resets or warns of account suspension
- Generic greeting (e.g. "Dear user"), grammar errors, branding inconsistencies

2

PayPal Phishing

- Claims your account is suspended, or that you've been "paid too much"
- Contains links to fake login pages
- Often no customer name, urgent tone, suspicious address

3

Amazon Phishing

- Claims order problems, locked accounts, prompts to update payment info
- Pressures user to act quickly
- Again, generic greeting, suspect sender, bad grammar

Phishing Email Example Types (Part 2)

4. Google Docs / Shared Document Scams

- Email says someone shared a document with you
- Includes link to a fake Google login page
- Unfamiliar sender, urgency, mismatched email address

5. IRS / Tax Scams

- Promises a refund or claims mistakes made in your favor
- Asks for SSN, personal data
- Note: legit IRS communications don't request personal info by email

6. Suspended Account Phishing

- Claims an account (Netflix, PayPal, etc.) is suspended
- Demands you "verify" or "update" your info via link
- Look for misspellings, missing recipient name, broken "To:" fields

Phishing Email Example Types (Part 3)

1 Unusual Activity Alerts

- Emails warning of suspicious login or usage
- Prompt to click to verify
- Check the actual links, ask: did you do anything unusual?

2 CEO / Executive Phishing (Business Email Compromise)

- Email allegedly from CEO or senior exec
- Requests urgent wire transfer or data access
- Sender address vs. display name mismatch, pressure tactics

3 Fake Job / Employment Phishing

- Promises high pay for little work
- Asks for bank account, SSN, or upfront "application fees"
- Attachment or link may contain malware

4 Apple / iCloud / App Store Phishing

- Warns of account issues, prompts for login via link
- Claims you have an unusual Apple billing issue
- Doesn't use your name, sometimes claims fictitious plans



Common Red Flags

- Generic greetings ("Dear customer" vs your name)
- Grammar / spelling / weird phrasing
- Suspicious sender address / domain typos (e.g. "appel.com" instead of "apple.com")
- Hover over links to verify URL (don't click blindly)
- Requests for personal info (passwords, SSN)
- Blurry / low-quality logos or images
- Pressure / urgency ("Your account will be closed in 24 hours!")

Spot the Scam: What to look for

How To Identify a Phishing Email

Subject You've won a \$1000 gift card!

Too-good-to-be-true offers



Giftcardsdirect.com <giftcardsdirect.com to me >

Discrepancies between the sender's name and email address



Suspicious links

[Click here to redeem](#)

Deer customer,

Spelling or grammatical errors

You are the winner of our \$1000 gift card giveaway.

Please login below to redeem your prize in the next 24 hours.

Demands urgency

[Log in now](#)

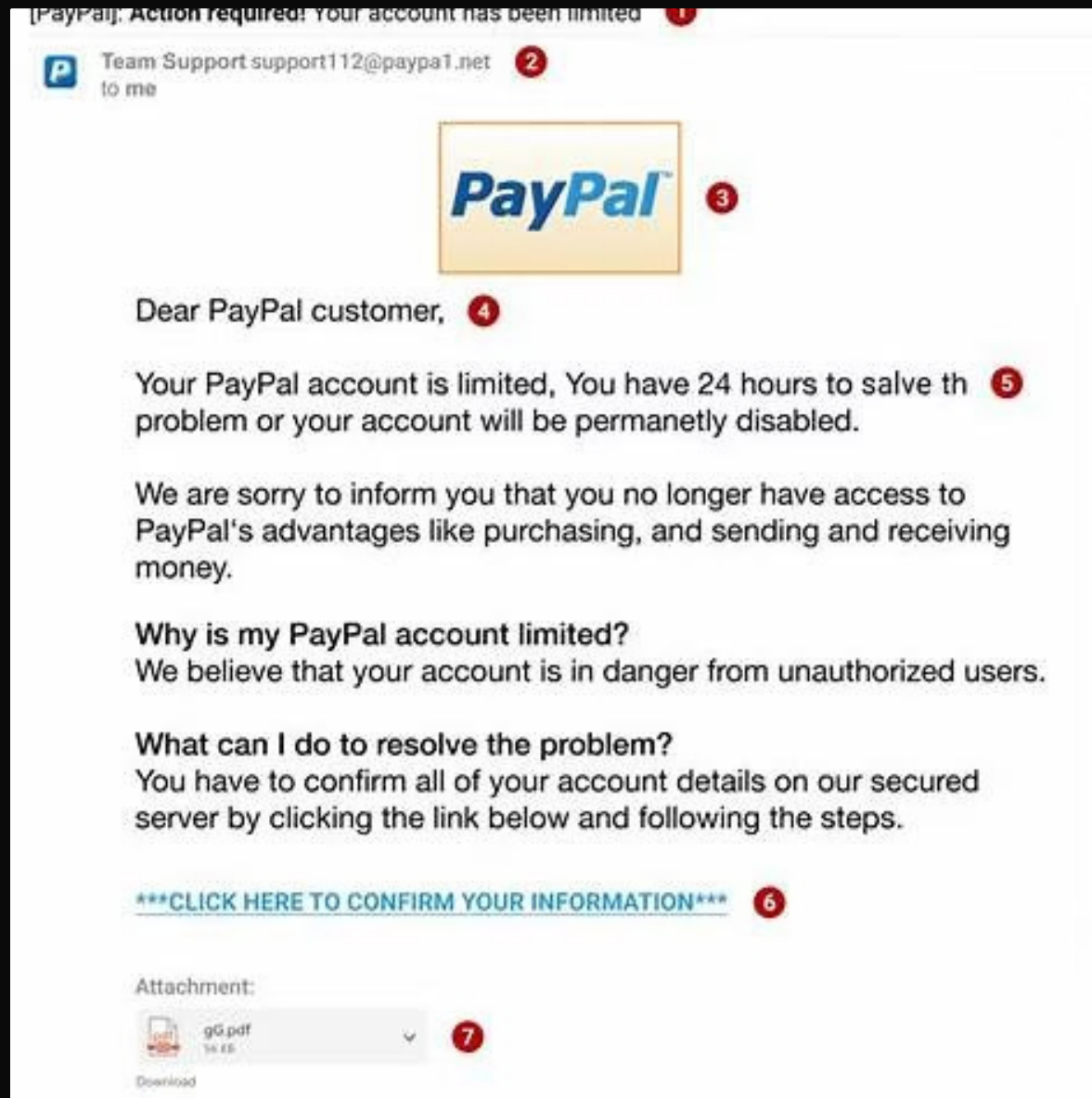
Requests sensitive information



digital gift card.png

Suspicious attachments

Spot the Scam: What to look for



Spot the Scam: Which Email is Fake?



UPGRADE SUBSCRIBER

Customer Support

Dear LINKEDIN Customer,

We're currently upgrading our systems to bring enhanced features to your LINKEDIN Account experience. As a result, your account is temporarily unavailable.

Please Note: this upgrade your LINKEDIN Account to our new system.

Note: FAIL TO UPGRADE YOUR ACCOUNT, IT WILL BE AUTOMATICALLY CLOSED.

After this step, you are permitted to access your LINKEDIN Account

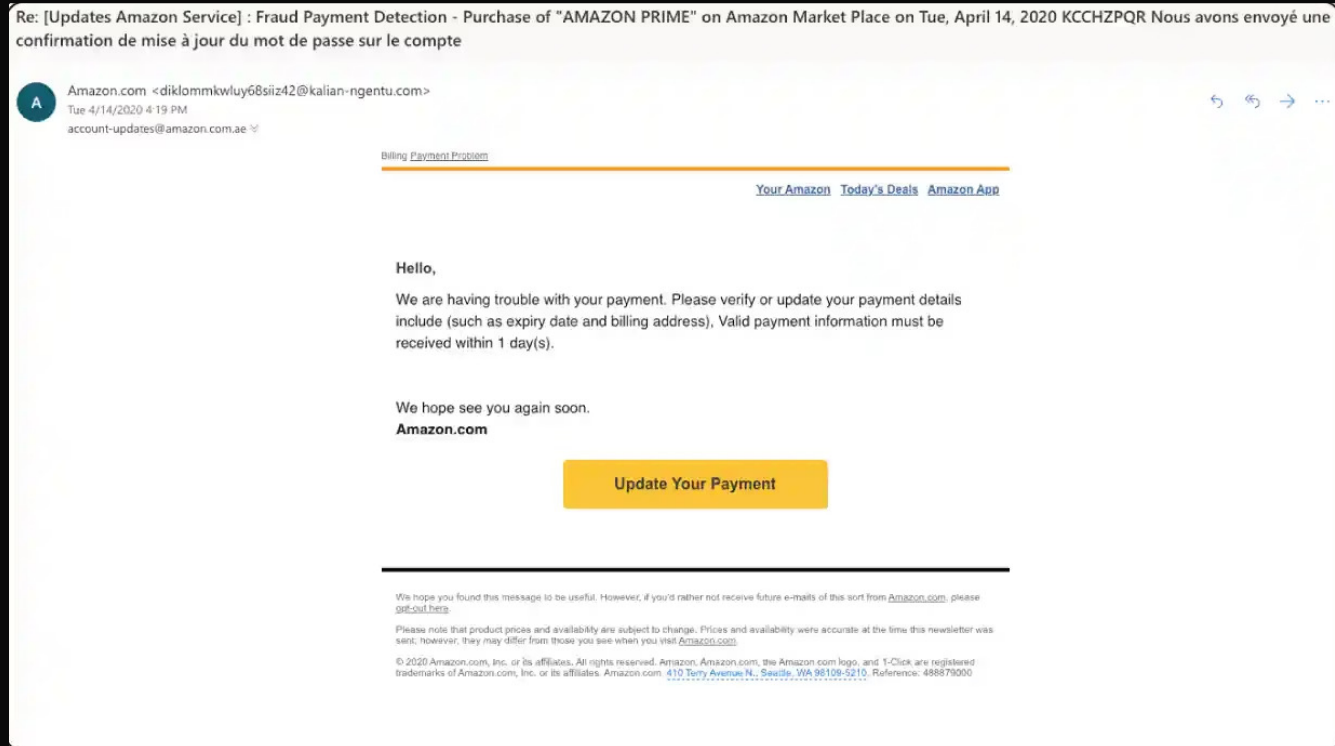
We've upgraded your protection on LINKEDIN and will continue to enhance your account security. To help us verify your account on our servers, please complete the following information requested . (1) E-mail :_____ (2)Password: _____ (3)Confirm Password:_____ After completing your account verification, your LINKEDIN account will not be interrupted and it will continue working as normal.

Sincerely,

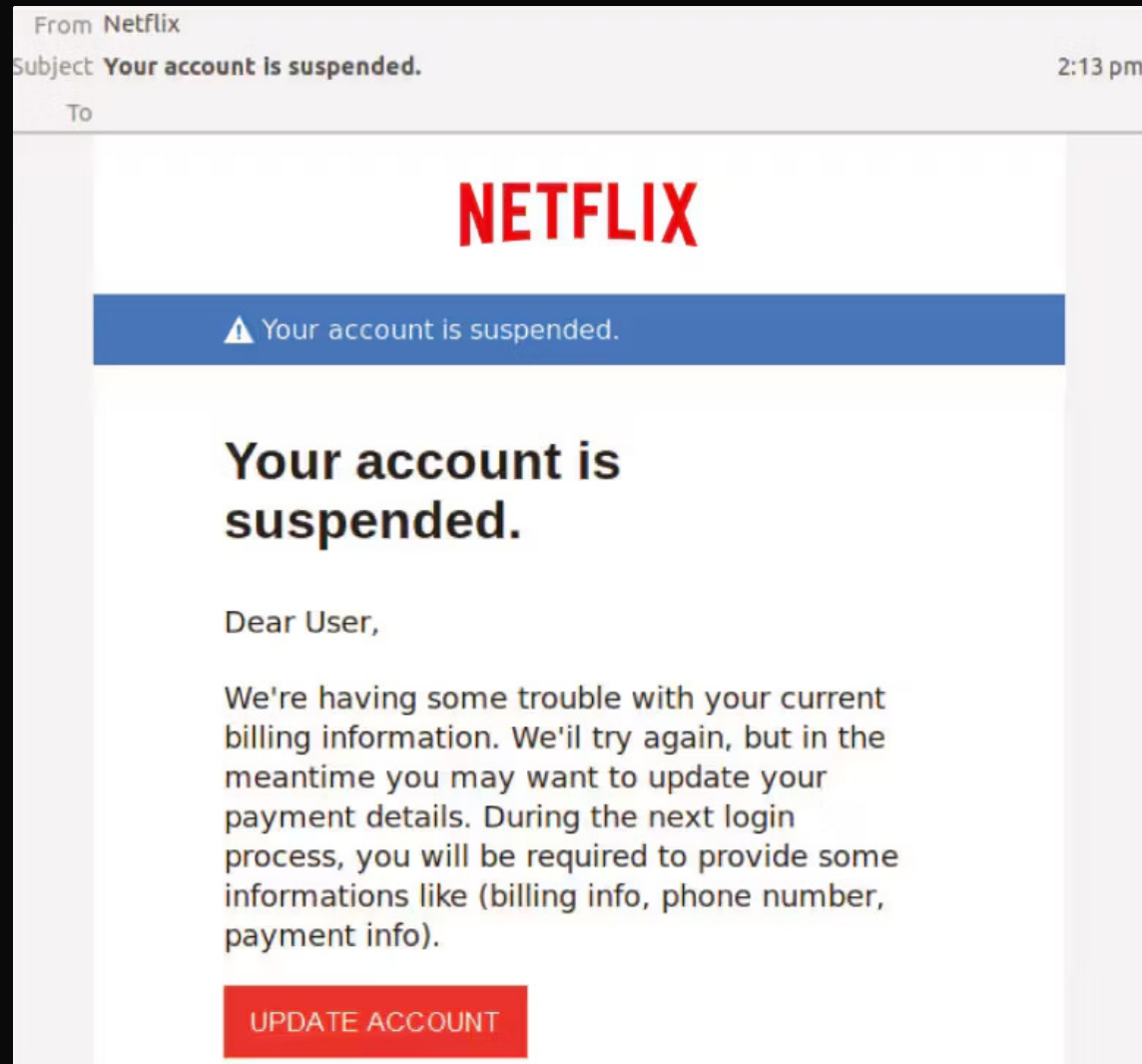
Customer Service Team.
Copyright © 2015 LINKEDIN.

[Reply to UPGRADE](#)

Spot the Scam: Which Email is Fake?



Spot the Scam: Which Email is Fake?



So, which one was fake?

All of them.

How to Stay Safe (The 6-Point Safety Plan)

1 Slow down

Don't click on urgency-based messages.

2 Check the sender

Look at the actual email address.

3 Hover before you click

See where links go.

4 Update passwords often

Use a password manager.

5 Enable 2FA (two-factor authentication)

Everywhere.

6 Use AI or filters

To block junk + phishing attempts.

"You don't need a firewall expert. Just follow smart habits."

What to Do If You Click / Are Already Affected



Change your password immediately (use strong, unique password)



Enable 2-Factor Authentication (2FA) on accounts



Run antivirus / malware scans



Report the phishing email (e.g. to FTC, Anti-Phishing Working Group)



Notify financial institutions / freeze credit, if sensitive data was exposed

Stay Vigilant & Protect Yourself

Best Practices

- Take emails urging urgent action with skepticism
- Always verify directly (go to website manually, **don't click link**)
- Use security tools (antivirus, email filters, anti-phishing tools)

Remember

- Educate others — coworkers, friends, family
- Even good security software can't prevent all attacks — vigilance is key



BONUS TOOLS + FREE ACCESS

You get free access to:



WonderWerx Community
(tools, trainings, checklists)



AI Essentials Course



Checklist: Post-Phishing Incident Response



E-Book: 21 Lies Hackers Want You To Believe

Scan the QR code on the next slide



WONDERWERX



Comment, "I met you at MICA"