Think Like a Hacker, Act Like a Pro: Real-World Security Tips for Health Clinics

Damien
Zanda Co-Founder &
Head of Customer Success

Paul
Zanda Co-Founder &
Chief Technology Officer

Introductions

Meet your speakers!

Damien

Zanda Co-Founder &
Head of Customer Success

+ Registered psychologist

+ Co-founder of psychology group private practice

Paul

Zanda Co-Founder &
Chief Technology Officer

+ Engineer

+ Founder of a successful technology advisory company

What We'll Be Covering Today

1. Why Security & Privacy Matters
2. Legal & Regulatory Foundations
3. Common Risks in Practice Settings
4. How to Spot Phishing Emails
5. What is Social Engineering
6. What You Can Do to Protect Yourself
7. The Ongoing Nature of Security
8. The Role of Key Technology Providers
9. Smart Use of Zanda in Your Practice

Why Security & Privacy Matters

Who this is for: practice owners, managers, and team members

The **threat landscape** is changing and rising every day

The link between patient trust, security, and professionalism

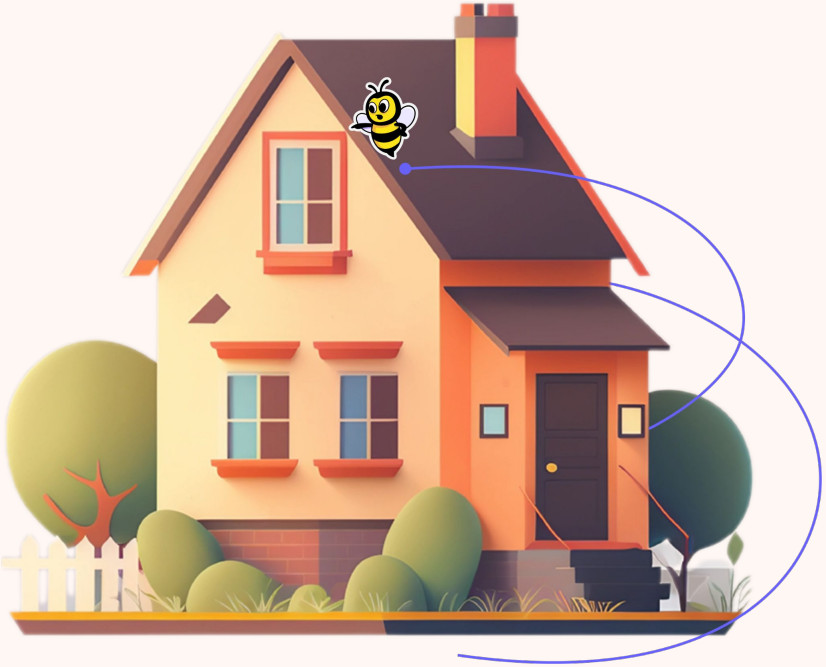
Legal & Regulatory Foundations

Global frameworks that influence best practice:

- HIPAA (US) & CCPA (California)
- PIPEDA (Canada)
- Australian Privacy Act & APPs
- New Zealand Privacy Act 2020
- GDPR (EU & UK)
- ISO 27001

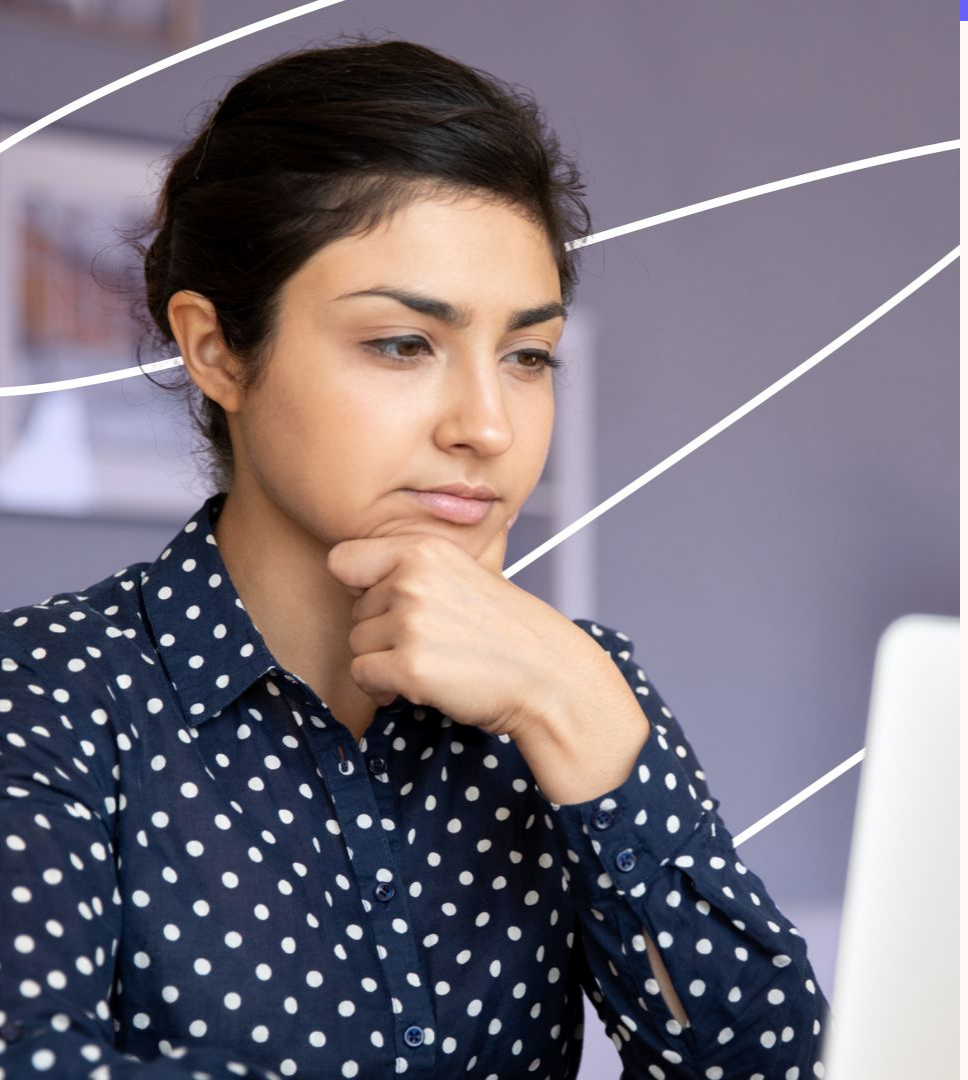
BEFORE YOU LEAVE HOME...

Lock All the Doors & Windows!



Common Risks in Practice Settings

- ⚠️ Human error
- ⚠️ Phishing and social engineering
- ⚠️ Weak passwords and shared logins
- ⚠️ Third-party software risks
- ⚠️ Lack of visibility over user activity



Typical Signs of a Phishing Email

- **Urgent** or **threatening** language
- Requests for **confidential information**
- **Unexpected attachments** or links
- Slight **misspellings** (e.g., paypa1.com instead of paypal.com)
- **Generic greetings** (“Dear Customer” instead of your name)

Common Goals of Phishing Emails

Stealing **login credentials** (for email, banking, work systems)

Collecting **personal information** (phone numbers, credit card details)

Spreading **malware** or **ransomware** through attachments or links

Getting the victim to make **unauthorized payments**

HOW TO SPOT PHISHING EMAILS

Payment Demand Phishing

Always check that the sender's name and email is correct and familiar

Carefully check the vendor email and name

Cross check the business name and address on Google Maps

Be suspicious of urgent language that pushes you to pay quickly

Request

Fiona Adler
to accounts@zandahealth.com

9 Jun 2025, 10:00 (10 days ago)

Could you please take care of the attached invoice now? Please set up the vendor and make payment.

Regards,
Fiona Adler

---------- Forwarded message ---------
From: Billing Department <ar@bizconsultingteam.com>
Sent: Friday, 6 June, 2025, 10:07 AM
To: Fiona Adler
Subject: Payment Reminder!INV 430584

This is to let you know that there is still an unpaid invoice 430584, which has been issued and attached for some time. Please give the settling of this invoice top priority.

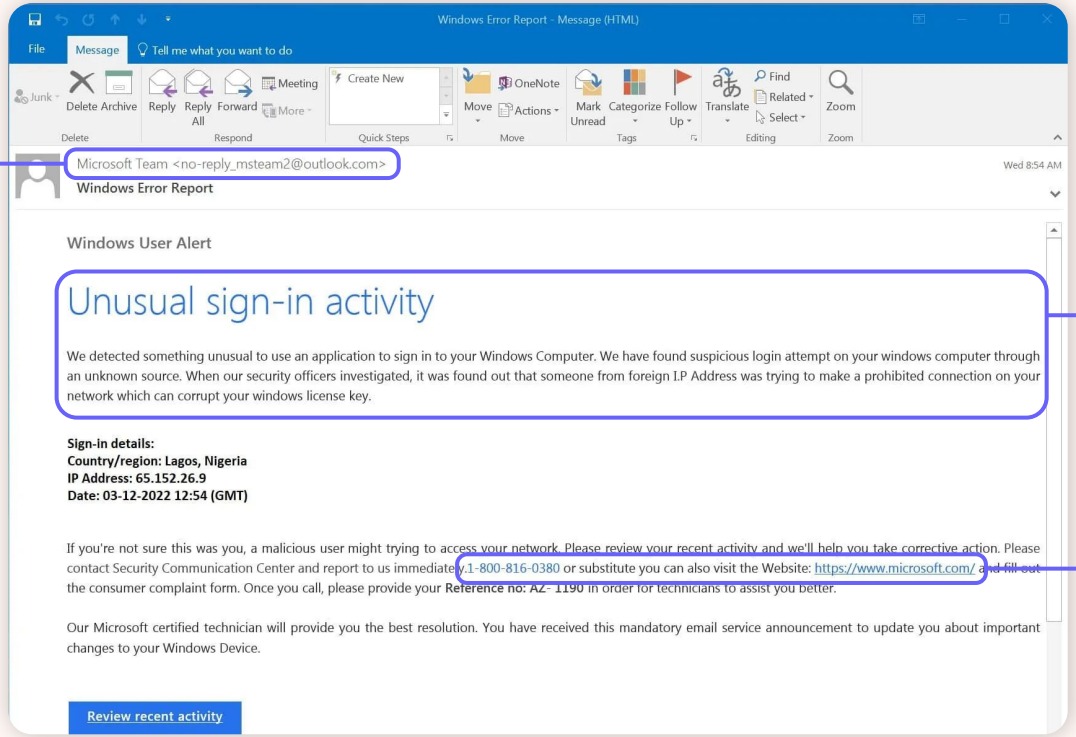
Should you require any assistance or have any questions regarding the outstanding invoice, please do not hesitate to contact us promptly.

Thank you.
Billing Department
100 Miller St,
North Sydney NSW 2060
ar@bizconsultingteam.com

HOW TO SPOT PHISHING EMAILS

Credential Phishing

Weird or misspelled email address or domain name



Threatening language ("Unusual sign-in activity") that evokes panic or fear

Do not click, but hover over all links to see and verify the URL

zanda

Zanda Talks Webinar

What is Social Engineering?

Social engineering: The manipulation of people into giving up confidential information or access, often without realizing it

Examples: Fake IT support, impersonating patients or staff

Techniques: Urgency, fear, sympathy, authority

SOCIAL ENGINEERING

Example 1

⚠️ **Context:** Someone calls claiming to be from a health industry directory (e.g., a Medicare listing, insurance database, etc.). They say they're "verifying your profile" and ask for full name, date of birth, provider number, and clinic address.

💡 **Why it Works:** Sounds legitimate, and the request seems harmless—but it's enough to commit identity fraud or spoof a clinic.

SOCIAL ENGINEERING

Example 2

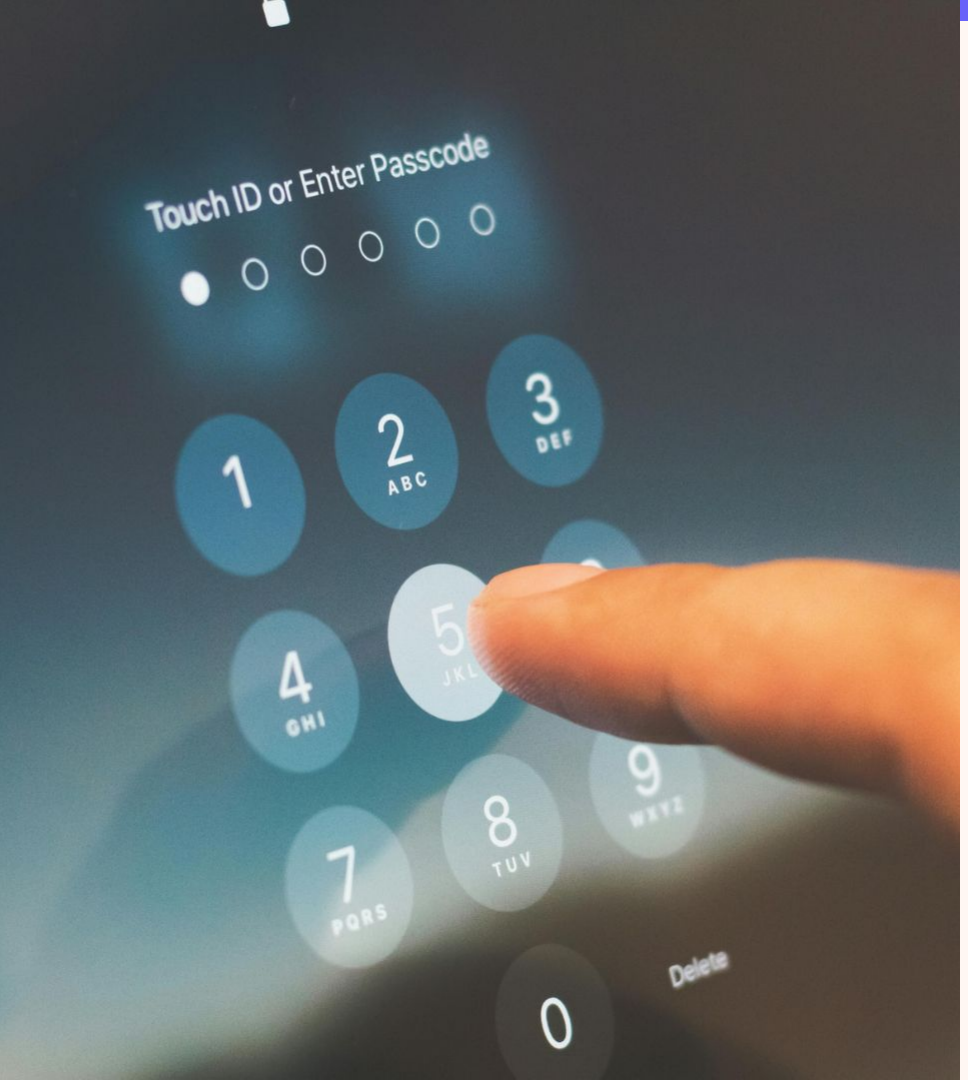
⚠️ **Context:** A receptionist receives a call from someone claiming to be “Dr. Sarah Miller from Riverdale Clinic.” The caller says a patient, Jane Watson, has just arrived in a distressed state and doesn’t have her latest treatment records. She urgently requests Jane’s full medical summary be emailed to dr.miller.requests@gmail.com, saying it’s a time-critical clinical situation.

💡 **Why it Works:** The request sounds medically urgent, invoking patient safety, and health staff are naturally inclined to trust and help fellow clinicians. The caller uses professional language. Personal email doesn’t trigger suspicion under pressure.

WHAT YOU CAN DO

System-Level Protections

- Enable **2FA or passkeys** on all systems (including Zanda)
- Use **strong, unique passwords** for every system
- Keep passwords secure with a **password manager**
- Restrict who can install software or access **admin settings**



WHAT YOU CAN DO

Device & Physical Security

- Password-protected screensavers & phone locks
- Secure laptops/PCs to desks where appropriate
- Remote lock & destruction
- Avoid placing printers or physical files in public areas
- Keep Wi-Fi networks password protected & private

WHAT YOU CAN DO

Staff Awareness & Security Culture

- Talk about security regularly, not just during onboarding
- Share examples of phishing emails or security incidents with your team
- Encourage safe behaviors, not shortcuts
- Perform background or police checks where appropriate

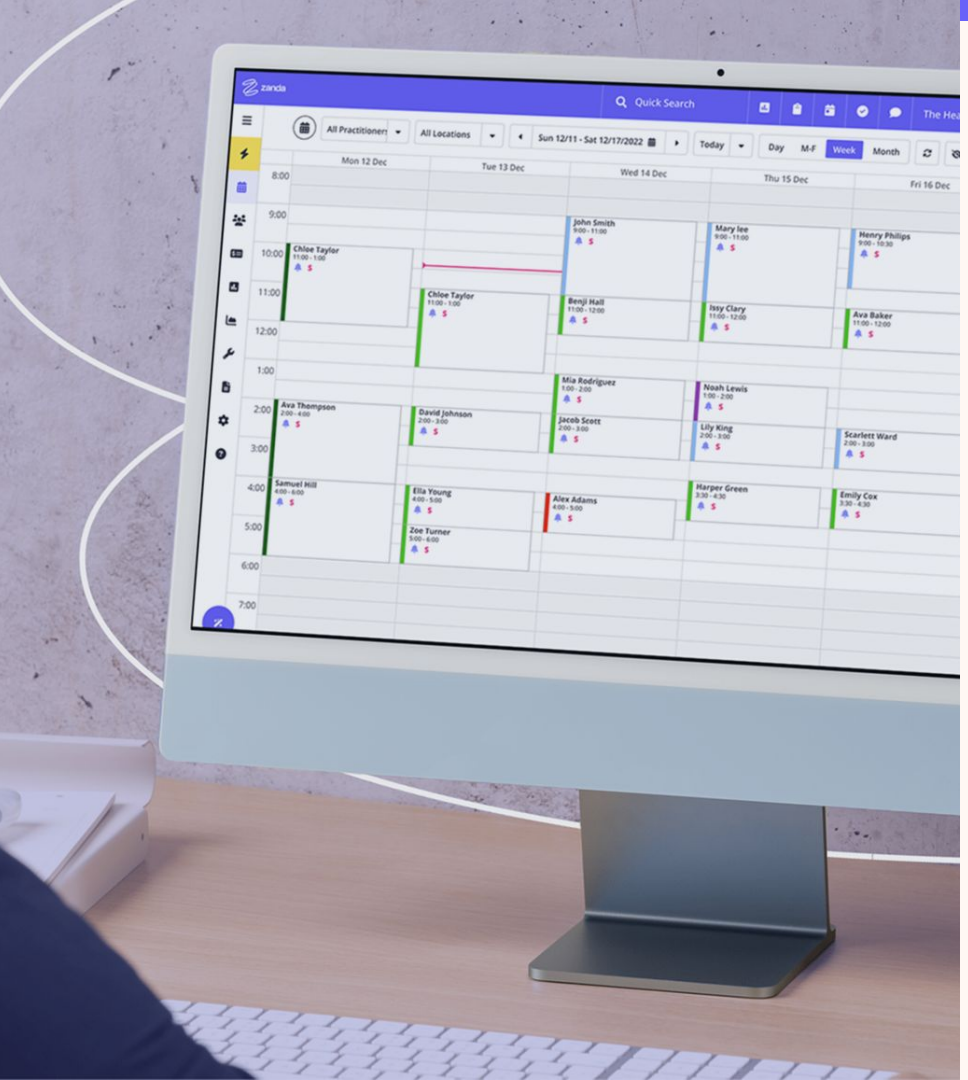
WHAT YOU CAN DO

Communication With Patients

- Use encrypted portals
- Use systems tailored for healthcare (not general software)
- Avoid using personal email or phones
- Ensure information received from contact forms on your website is stored securely

Security is Ongoing

- Schedule annual privacy and security reviews
- Rotate passwords
- Audit access
- Monitor updates from industry bodies
- Continuous improvement approach

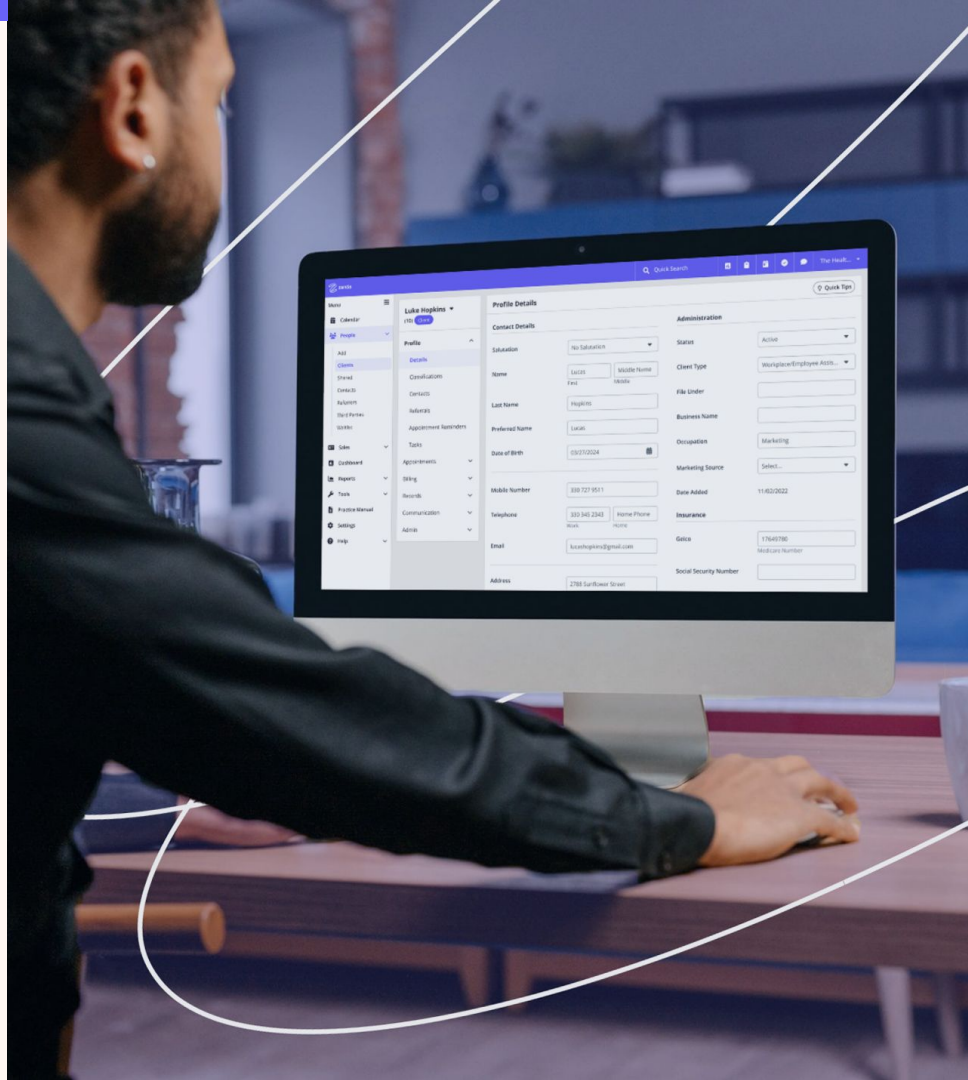


The Role of Key Technology Providers

- Secure infrastructure & development practices
- External vulnerability & penetration testing
- Ongoing monitoring
- Secure-by-design approach (including AI features)
- Assess the privacy & security posture of third-party vendors
- Independent data protection officers & security officers
- Security management system
- Externally audited (e.g., ISO 27001, SOC 2)

Quick Reminders for Secure Use of Zanda

- Ensure each staff member has a unique user account
- Enforce 2FA for all users
- Limit access through user permissions
- Use privacy mode when at risk of someone seeing your screen
- Log out when away from your desk
- Regularly review and remove unused accounts (e.g., ex-staff)
- Run periodic spot-checks using the activity logs



Zanda Announcements

Aha Ideas Board

To add an idea from your Zanda account: go to **Help > Submit Idea**

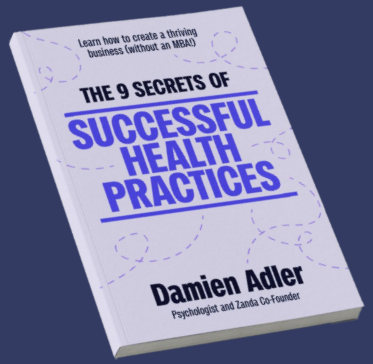
Zanda Academy

Get the most out of Zanda with Zanda Academy courses at: **academy.zandahealth.com**

Zanda Book

We've written a book about how to run a successful health practice!

Stay tuned for updates on the release date.



For More Information & Resources

Email

Get in touch with us at **support@zandahealth.com**

Website

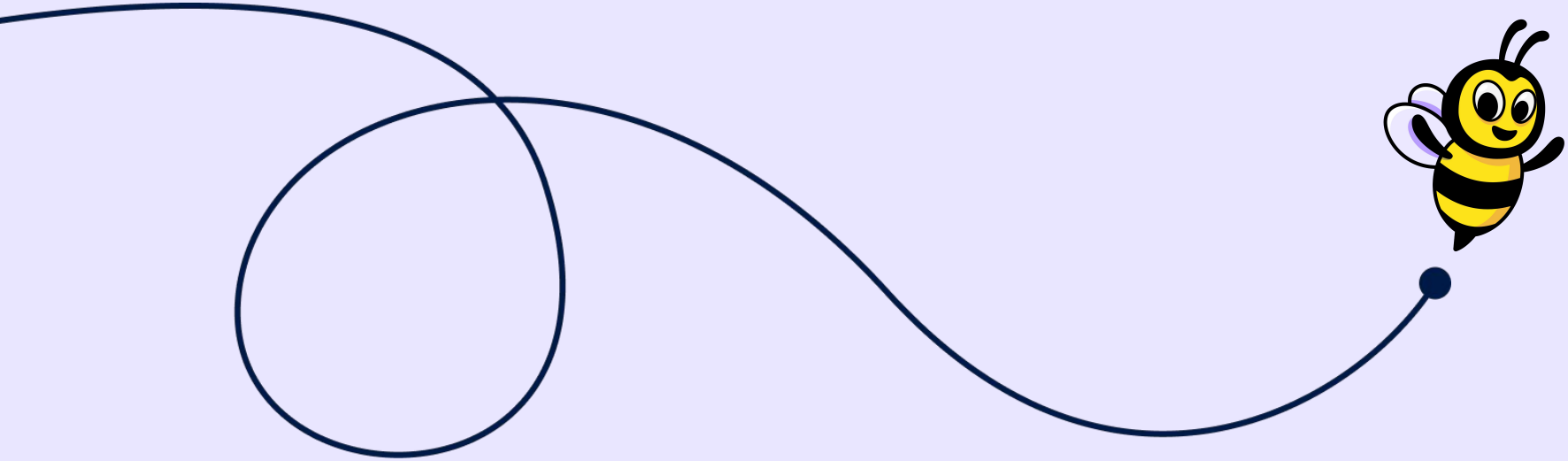
Visit us at **zandahealth.com** for support resources

Support Call

Book a **live call** (video or phone) from our website or directly from your account

Practice Hive

Check out the **Zanda Practice Hive** to stay up-to-date with the latest information



Thank you for listening!

zanda