KingPhisher - User Guide

What is KingPhisher?

KingPhisher is a chrome browser extension that helps you spot phishing emails.

It works directly in Gmail, Outlook, Yahoo Mail, Yandex Mail, and ProtonMail. When you open an email in a chrome-derived browser (like Chrome, Brave, Edge, Opera, Vivaldi, Arc), KingPhisher analyzes it and gives you a risk score from 0 to 100, along with a breakdown of what it found suspicious.

Think of KingPhisher as a second pair of eyes, not a judge. It doesn't make decisions for you. It shows you what to look at so you can make better decisions yourself.

Privacy

KingPhisher runs entirely on your computer. Your emails, sender addresses, subjects, and content never leave your browser. There is no server, no cloud storage, and no data collection. The only external communication is checking for extension updates through the Chrome Web Store.

How It Works

1. **Install the extension** from the Chrome Web Store
2. **Open any email** in Gmail, Outlook, Yahoo, Yandex, or ProtonMail
3. **A risk banner appears** in the corner with a score from 0-100
4. **Click the KingPhisher icon** in your toolbar for full details and explanations

Everything happens inside your browser. No data is sent anywhere, ever.

Understanding Your Risk Score

Score	Level	What It Means
0-44	🟢 Low Risk	Few or no suspicious indicators found
45-74	🟡 Medium Risk	Some suspicious elements - review carefully
75-100	🔴 High Risk	Strong phishing indicators - be very cautious

What KingPhisher Checks

Sender Identity

- Does the sender name match the email address?
- Is the email from a free service (Gmail, Yahoo) but claiming to be a company?
- Does the domain use lookalike characters? (e.g., "paypal.com" with a capital I)
- Is the sender address and/or domain random or gibberish?

Email Content

- Generic greetings like "Dear Customer" instead of your name
- Urgency language ("Act now!", "Within 24 hours", "Account suspended")
- Financial pressure ("Invoice overdue", "Payment required")
- Poor grammar, excessive punctuation, ALL CAPS

Links

- Does the visible link text match where it actually goes?
- Are there shortened URLs hiding the real destination?
- Do links use IP addresses instead of domain names?

Attachments

- Dangerous file types (.exe, .vbs, .js, .bat, .scr, .lnk)
- Password-protected archives (often used to hide malware)
- Double extensions like "invoice.pdf.exe"

Important Limitations

KingPhisher is a guideline, not a guarantee. Please understand these limitations:

False Positives (Legitimate Email Scored High)

Some perfectly safe emails may get a high score. Common causes:

- **Newsletters** with tracking links (shortened URLs, mismatched display text)
- **Corporate emails** sent through third-party services (triggering "via" warnings)
- **International emails** with non-English characters
- **Automated notifications** with generic greetings

If a legitimate email scores high, review the findings. You'll often see that the flagged items are normal for that type of email.

NOTE: If you have multiple webmail windows open or other extensions that modify the DOM structure of the webmail page (e.g. ad-blockers), KingPhisher may not be able to analyze or find the correct email. If this happens, be sure to de-activate the conflicting extensions and then open KingPhisher to click on “Reset & Re-Scan”.

False Negatives (Phishing Scored Low)

A sophisticated spear-phishing email might score low if:

- The attacker uses a convincing domain that closely matches a real one
- The email is personally addressed to you with your actual name
- The language is well-written with no obvious urgency keywords
- There are no attachments or suspicious links

A low score does not guarantee an email is safe.

What KingPhisher Cannot Do

- It cannot check if links lead to actual phishing sites (that would require visiting them)
- It cannot scan inside attachments for malware
- It cannot verify SPF/DKIM/DMARC email authentication (requires server-side lookups)
- It cannot guarantee detection of every phishing email

Best Practices: Use Your Judgment

KingPhisher works best as part of your own security routine:

1. **Check the score** - Is it green, yellow, or red?
2. **Read the findings** - What specifically looked suspicious?
3. **Think critically** - Does this email make sense? Were you expecting it?
4. **Verify independently** - If your bank emails you, call your bank. Don't click the link.
5. **Trust your instincts** - If something feels off, it probably is.

Quick Tips for Staying Safe

- **Hover over links** before clicking to see where they really go
- **Never open attachments** you weren't expecting
- **Don't trust urgency** - real companies don't threaten you over email

- **Use a password manager** - it won't autofill on fake websites
- **Enable two-factor authentication** everywhere you can
- **When in doubt, contact the sender** through a different channel

Auto-Scan Toggle

By default, KingPhisher automatically scans emails when you open them. If that gets overwhelming, you'd opt for manual scan and selectively pick the emails that look suspicious for additional analysis:

1. Click the KingPhisher icon in your toolbar
2. Scroll down to the **"Auto-scan emails when opened"** checkbox
3. Uncheck it to disable automatic scanning
4. Click **"Scan Again"** whenever you want to analyze an email

Remember: KingPhisher is just a tool to help you see what's hidden inside an email. The final decision is always yours. Stay safe, stay vigilant, and trust your judgment.