



Phish Free



What is INKY?

INKY is a phishing prevention and education tool that uses banners at the top of emails to inform users of the security status for inbound emails and malicious links.

When you receive an email, you can expect to see a banner like the three examples below, depending on the security status.

GRAY BANNER "SAFE":

Inky Phish Fence has analyzed this message.
(From: from@example.com, Internal)

[Report This Email](#) [FAQ](#) [Protection by Inky](#)

This mail has gone through INKY's , and does not see any threats.

YELLOW BANNER "CAUTION":

Caution (External, from@example.com)
Blacklisted Domain [Details](#)

[Report This Email](#) [FAQ](#) [Protection by Inky](#)

Indicates that INKY found something unusual about the email message. It is not necessarily phishing or dangerous but something you should be aware of. For example, one of the categories for a message to be marked as unusual is "Sensitive Content". This may flag emails containing financial information or contain a request for sensitive personal information. Messages with this flag should be given extra scrutiny, but may not necessarily be malicious.

INKY[®]

Phish Free



RED BANNER – “DANGER”:

Danger (External, from@example.com)
Malware Attachment [Details](#)

[Report This Email](#) [FAQ](#) [Protection by Inky](#)

This banner indicates that INKY thinks the message is suspicious and likely to be phishing or dangerous in some other way. This includes brand impersonations (e.g., a fake “account alert” email from your IT department), blacklisted phishing URLs, or attempts to spoof mail to look like it came from an internal company account.

The malicious email banner will contain information about why the email has been flagged as such. You can read more about why INKY determined that it was risky by clicking the “**Details**,” link.

Reporting “Phishy” Emails:

You can actively help by identifying and reporting phishing attempts, so that INKY learns to flag these in the future, and these cyber criminals can be stopped.

To do this, click on the “**Report This Email**,” link below any INKY banner.

Danger (External, from@example.com)
Malware Attachment [Details](#)


[Report This Email](#) [FAQ](#) [Protection by Inky](#)

This will take you to the Report this email page which will ask you to choose how you want to classify this email. Click on **Safe**, **Spam** or **Phishing** and hit submit at the bottom.

INKY[®]

Phish Free




Inky Phish Fence: Report This Email

From:
Subject: FW: [External] Change your password immediately. Your account has been hacked.
Inky Result: Danger (Bitcoin Blackmail Scam, Sensitive Content)

Choose the correct label for this message:

Safe

Spam

Phishing

Contact email:
(Pre-filled with the first recipient in your organization.)

Optional comment:

Send raw message for analysis.


Oops I clicked on a shady link:

If you click on a link inside a suspicious message INKY will supply you with a screenshot of the webpage of the malicious link, a description of why the link is categorized as malicious and two additional navigation options, 1) Proceed to the site 2) Do not proceed.

INKY[®]

Phish Free





Inky Phish Fence: Link

You clicked a link in an email processed by Inky Phish Fence.

The link will take you to: <https://click.email.microsoftemail.com/...>


Inky classified the message containing this link as dangerous. [Details](#)

Visiting this site may not be safe. Are you sure you want to proceed?

[Proceed to Site](#)
This may not be safe

[Do Not Proceed](#)
[Learn more about Inky](#)

Screenshot of linked site:



Microsoft Privacy Statement

Last Updated: October 2018 [What's new?](#)

[Expand All](#)

[Print](#)

Your privacy is important to us. This privacy statement explains the personal data Microsoft processes, how Microsoft processes it, and for what purposes.

Microsoft offers a wide range of products, including server products used to help operate enterprises worldwide, devices you use in your home, software that students use at school, and services developers use to create and host what's next. References to Microsoft products in this statement include Microsoft services, websites, apps, software