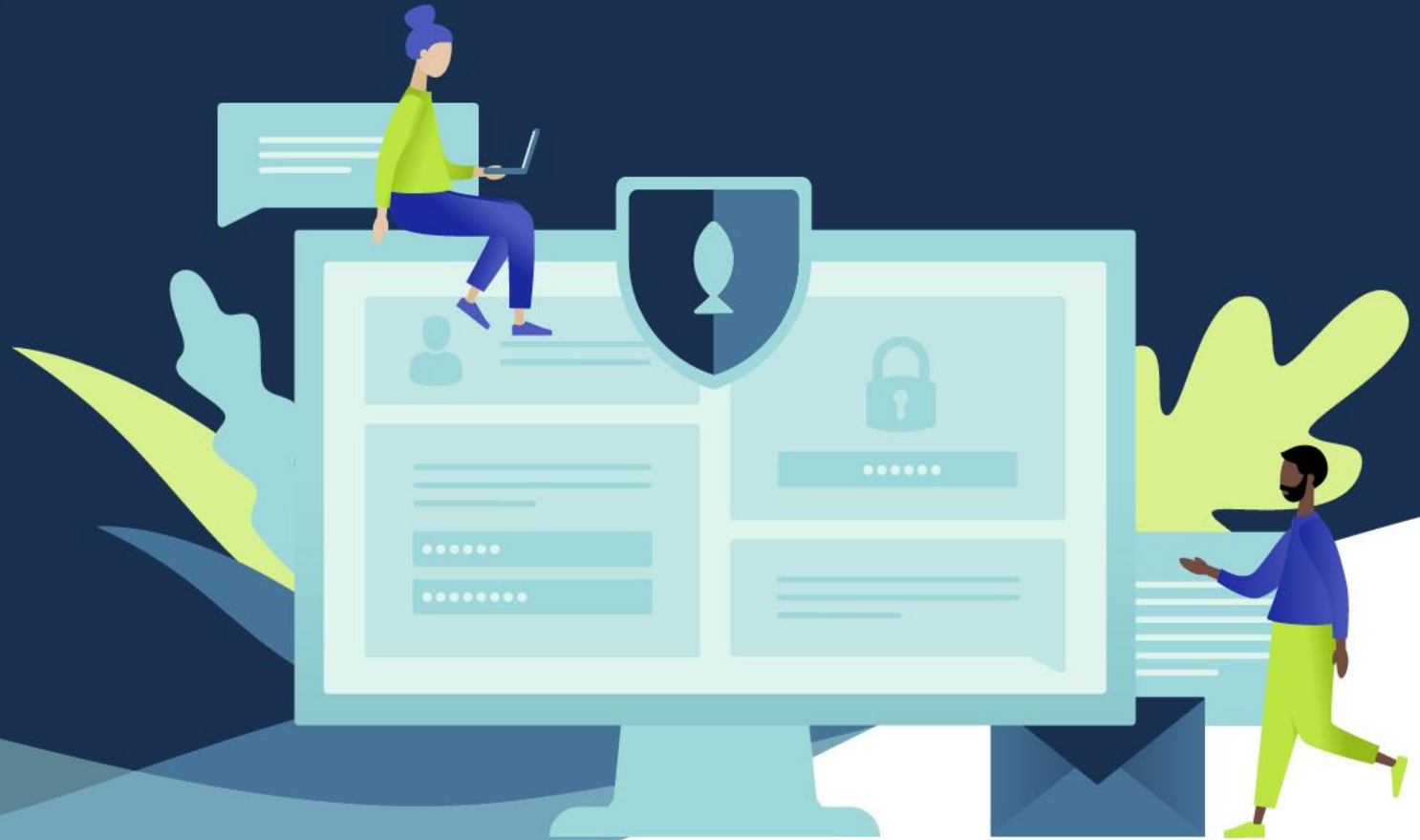# Phriendly Phishing

Using Email Templates to Elevate Your Phishing Simulation Training

We will commence shortly...

Phriendly Phishing

Special Guests:

Have a Question?
Use the Q&A feature during the webinar to ask your questions along the way!

Benji Zorella
eLearning Designer

Seth Saunders
Sales Engineer

Today's Agenda

- Anatomy of a Scam
  - Purpose of branded templates
  - Purpose and how to use tag management

- Tips & Tricks for creating an email template
  - Optimise the mobile experience (100% widths)
  - Manipulate tables and individual cells
  - Using liquid code to create sophisticated and variable emails

- Resources to support crafting your phishing templates

Have a Question?
Use the Q&A feature during the webinar
to ask your questions along the way!

The Anatomy of a SCAM

- How do scams work?

- What makes an effective SCAM email?

- What are branded templates, and why would you use them?

Have a Question?
Use the Q&A feature during the webinar
to ask your questions along the way!

The Anatomy of a SCAM

Most scams follow the same pattern and once you understand this, the tricks of the scammer become *easier to spot*.

1. The Approach

Convincing & Persuasive!

When scammers approach you it will always come with a **story** designed to make you believe a **lie**.

The scammer will pretend to be something they are not, a government official, an expert investor, a lottery official or even a romantic admirer.

The Anatomy of a SCAM

Some scams don't need to hack computers, they focus on hacking humans.

2. A Scammer's Toolkit

They use your personal details to make you believe you have **dealt with them before** and make the **scam appear legitimate.**

Scammers love to create a sense of **urgency**, so you don't have time to think things through and react on emotions rather than logic.

A scam can have all the hallmarks of a **real business** using high quality graphics with technical industry jargon.

They play with your **emotions** by using the **excitement** of a win, the promise of everlasting **love**, garnering **sympathy** for an unfortunate accident, eliciting **guilt** about not helping or causing **anxiety** and **fear** of a fine or an arrest.

Similarly, they use high pressure sales tactics saying it is a limited offer, prices will rise, or the market will move; **anything** to get you to think the **opportunity will be lost.**

The Anatomy of a Phishing Email

Phriendly Phishing aims to educate with empathy.
We train, not trick.

1. Convincing Sender information

- Using personalisation and advanced variables can make this FAR harder to detect for lower-level learners.

2. Compelling Subject lines

- They use personal details to make victims believe they have **dealt with them before** and make the scam **appear legitimate**.

- They play with your **emotions** by using the **excitement** of a win, the **promise** of everlasting **love**, **sympathy** for an unfortunate accident, **guilt** about not helping or **anxiety** and **fear** of arrest or a fine. All play on a sense of **urgency.**

3. Convincing email Content

- Does the content elicit an **emotion**?

- Is it **personalised**?

- What **demographic** of learner is likely to click on this email?

Branded Templates

Credibility and Familiarity

- Leverage the trust of an existing organisation/relationship with the end-user
- Use personal details to make victims believe you have dealt with them before and make the scam appear legitimate
- We use logos and brand identities to achieve this

Legality

Admins need to accept the Terms and Conditions for branded templates before they are unlocked on the Phriendly Phishing platform.

*You can filter on Unbranded to view <u>only</u> unbranded templates

Branded Templates

Top Performing Branded Emails (CTR):

- Kiwibank Visa statement – 71%
- TechSmith Gift Card 01 – 63%
- UK Law Firm Notification – 63%
- Amazon Sign-In – 62%
- Kathmandu NZ Sustainability-Clearance Sale – 61%
- Microsoft account password change – 58%
- Australia Post Review – 57%

AVERAGE BRANDED CTR 62%

Top Performing Non-Branded Emails (CTR):

- Traffic Infringement Notice V2 – 73%
- Smoking Area Update – 36%
- Appreciate the Help – 35%
- Leave Application – 35%
- Payroll Instruction Example – 35%
- Upcoming Training – 35%
- Change In Parking – 35%

AVERAGE BRANDED CTR 37%

CTR = Click-Through Rate
How is a template's Click-Through-Rate (CTR) calculated?
Total number of sends divided by the number of first unique clicks*
eg: 100 sends, 10 individuals click = 10% CTR

*individuals may click on the link several times, but CTR calculates on the 'first click'

Tag Management

- **Filtering Branded emails**

- **Filtering Emails based on Themes:**

Branding: All ⌄

🔍 Search

Clear selected items

☑ All

☑ *(Non Branded)*

☑ Branding

Themes: All ⌄

🔍 Search

Clear selected items

☑ All

☑ *(Blanks)*

☑ Accident

☑ Accomodation

☑ Account

Tips 'n Tricks

- Optimise the mobile experience (100% widths)

- Manipulate tables and individual cells

- Using liquid code to create sophisticated and variable emails

- HTML resources to support crafting your template creation

Have a Question?
Use the Q&A feature during the webinar
to ask your questions along the way!

CONFIDENTIAL

Demo Time!

Optimising the mobile experience
Using 100% width for tables and 85% width for content cells.

Editing Tables/Cells
Editing individual Table and Cell properties

Liquid Code Variables
Adding variables for targeting learners at scale (admins with sub-zones, take note!)
*more coming soon to a platform near you

Resources
Support you in crafting your phishing templates

HTML:

- Learn HTML with W3schools.com
  - HTML Table Sizes
  - Padding & Spacing
  - HTML Responsive
  - Dynamic sizing template will be made available to you in your zone's **Email Template Drafts**

Liquid Code Variables:
Coming soon

Branded Newsletters
A starting point for your branded templates:
Milled.com is a search engine for email newsletters

Questions?

support@phriendlyphishing.com
help.phriendlyphishing.com