“White Hat Phishing”
- lessons learnt
Steve, aka @snori74

- Defensive security guy, some Linux skills
- Spent years on email and spam
- Working for a small IT company
- A few clients with hundreds of staff
- Most under 100 - and many under 50
- Like a large organisation with several divisions

Ransomware -> “we need to train users”

...hence considering white hat phishing
Ethical issues

Fire drills? …not really because:

• No warning given
• No "this is a drill" re-assurance
• People will "fail" - perhaps sensitive, perhaps senior

Our approach:

• Authorisation from two senior staff
• No "shaming" of those caught out

We run "phishing" campaigns against ourselves to practice, and measure our level of caution
SaaS or not?

Many SaaS, and open source options

- SaaS for a smaller business 'doing it themselves'
- A user-friendly SaaS product still has a learning curve
- We thought we had the skills to self-host
- As consultants, the freedom was attractive
We chose ‘gophish’
Big hits - or little trickles?

Two contrasting approaches:

• One or two carefully crafted “phishes”
• A slew of low quality opportunistic scam emails

The first will catch many more staff, but:

➢ We aim to “innoculate” users
➢ Giving users practice at recognising malicious emails
➢ Testing that they handle them according to policy
Melissa Jones (friends with Katie) commented on a post that you're tagged in.

Melissa wrote: "Amazing stuff...!!"

Reply to this email to comment on this status.
To Spear or not?

A different approach to training and follow-up:

- It will be expensive
- Considerable time for each target
- A creative, ‘sneaky’ mindset is required

- These can feel very exploitative
- Around 50% of targets will "get caught"

...which is a lot of annoyed senior staff!
Who to pretend to be?

- It’s pointless to send NZ staff email "from" Wells Fargo
- Problems (!) with pretending to be ANZ or BNZ

We find facebook.com and linkedin.com catch plenty of targets...

...and far enough away that they don't hassle us!
Getting 'creds'

This is the *definition* of 'phishing', but...

**We no longer even *pretend* to do this, because:**

- A user clicking "Login page" has already been fooled
- If we collect creds then we need to guard them well
- A user has no way to verify our “pretend” capture
- Cred capture unnecessarily stresses the user
Tell them or not?

Good to give the user a *little* scare!

…and perhaps some brief training

Our “scare page”
- Tells them they have fallen for a “simulated phish"
- No harm has been done
- They should have been suspicious

**Training:**
- Was it from someone they didn't know?
- Was it 'out of character' in some way?
Please be careful with email

The email that led you here was sent as part of an Email Phishing Awareness Test run by CommArc Consulting Limited on behalf of Example Corp.

The test is designed to help you identify and avoid unsafe emails. It was carried out at the request of Anne Able, and the approval of Mr Ben Baker. Please contact them if you have any questions.

In this case, no harm has been done - but you need to improve your email habits.

This page is completely safe. However, it could just as easily have been a malicious attack designed to compromise your systems.

The email will have had some warning signs.

- It may have came from an unfamiliar sender.
- Was from someone you know - but was out of character
- It asked you to click on a link you weren't expecting to receive.
Our current approach:

- Written to be clear, simple and accessible
- Suitable to be sent to all staff
- Does not include details of "who fell"
- Has clear graph of performance
- Comparison with past tests

* Full technical logs are provided to management in Excel format
De-brief/training

• Make sure everyone has the results
• Ensure that internal policies are clear
• Half-hour "all hands" meeting - with Q&A
• Such "simulated phishing" is now standard
• We expect improvement over time

Most organisations have 30-50% "fail" rate initially
After two 'tests', this falls towards 10%

Because we use the same 'suite' of phishes for all customers, we can almost rigourously say that this is true.
‘gophish’ and ‘phishbuckets’

https://github.com/gophish

https://github.com/CommArc/phishbuckets

Phishbuckets

For use with ‘gophish’ from Jordan Wright

(Note: This is a work in progress - ‘gophish’ was at only v0.2.0 when this was written)

These scripts are based on a series of assumptions which are true for our own work. If these don’t match the way you do your phishing, then these scripts may not be for you...
• PhishMe / Cofense, SaaS
• KnowBe4, SaaS
• Duo Insight
• SANS Antiphishing Simulation
• King Phisher, OSS
• TrendMicro SaaS

All these differ considerably...
Questions?

Steve Brorens

@snori74