PHISH FOR THOUGHT: COMBATTING MODERN EMAIL THREATS
March 2020
Dr Steven Murdoch
Innovation Security Architect
OneSpan Innovation Center
Phishing is one link in a network intrusion chain – not the only point of defense

- **Reconnaissance**
  - Research, identification and selection of targets

- **Weaponization**
  - Develop malware to exploit security vulnerability

- **Delivery**
  - Transmit malware to targeted environment

- **Exploitation**
  - Trigger execution of malware to allow remote access

- **Installation**
  - Maintain persistent access to targeted environment

- **Command and Control**
  - Control targeted environment through the malware

- **Actions on Objectives**
  - Actually achieve end goal, e.g. steal or encrypt data

Hutchins et al. Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains
Phishing is nevertheless a significant problem

- In 2019, 55% of organizations fell victim to at least one successful phishing attack
- Rate of phishing attacks has decreased, which Proofpoint attribute to a quality over quantity strategy
- Top impacts include
  - Loss of data (53%)
  - Credential compromise (47%)
  - Ransomware infection (47%)
- Only 35% of organisations did not suffer a ransomware infection
  - 65% did, of which half paid the ransom
  - Of those who paid the ransom, 22% never regained access to their data

Results of survey of over 600 IT professionals, Proofpoint State of the Phish, 2020
UK fraud statistics now can quantify financial losses resulting from phishing

- Payment fraud (known as authorized push payments) often involves phishing, including where the email account is compromised
- Where criminals arrange for a legitimate business invoice to be paid to the wrong account accounted for £92.7 million over 3,280 cases in 2018
  - Average £28k per case
- Where the CEO of an organization is impersonated losses were £13.8 million over 519 cases in 2019
  - Average £26k per case

Peebles Media sued its employee Patricia Reilly to reclaim loses of £107,984

“[Reilly] stated she had not noticed that there were two email addresses. Given her ignorance of any other features of the transaction that suggested that a fraud was being practised on her and the apparently innocuous nature of the spurious email address, I am not convinced that this evidence demonstrates a breach of her implied obligation.”

Reilly lost her job; her line manager was demoted, the criminal was not caught.

Fraud the Facts 2019, UK Finance  Peebles Media Group v Patricia Reilly: Full case report, Scottish Financial News
NCSC propose a multi-layered approach to mitigating the harm of phishing

1. Make it difficult for attackers to reach your users (e.g. filtering, spoofing protection and reducing information)
   - Disrupt reconnaissance, weaponization and delivery stages of cyber kill-chain

2. Help users identify and report suspected phishing emails (e.g. training and creating culture of reporting)
   - Disrupt delivery stage

3. Protect your organisation from effects (e.g. anti-malware, patching and 2FA)
   - Disrupt exploitation and installation stages

4. Respond quickly to incidents
   - Disrupt C&C, and actions on objectives

“Training your users – particularly in the form of phishing simulations – is the layer that is often over-emphasised in phishing defence. Your users cannot compensate for cyber security weaknesses elsewhere. Responding to emails and clicking on links is a huge part of the modern workplace, so it’s unrealistic to expect users to remain vigilant all the time.”
– NCSC

“[Mock phishing] does little for security but harms productivity (because staff spend ages pondering emails, and not answering legitimate ones), upsets staff and destroys trust within an organisation.”
– Murdoch & Sasse

Ref: NCSC, Phishing attacks: defending your organisation
Murdoch & Sasse, Should you phish your own employees?