Research Institute
Cyber Defence
Universität der Bundeswehr München

Hooked: A Real-World Study on QR Code Phishing

Mavin Geisler, Daniela Pöhn, und Wolfgang Hommel

31. DFN-Konferenz “Sicherheit in vernetzten Systemen”

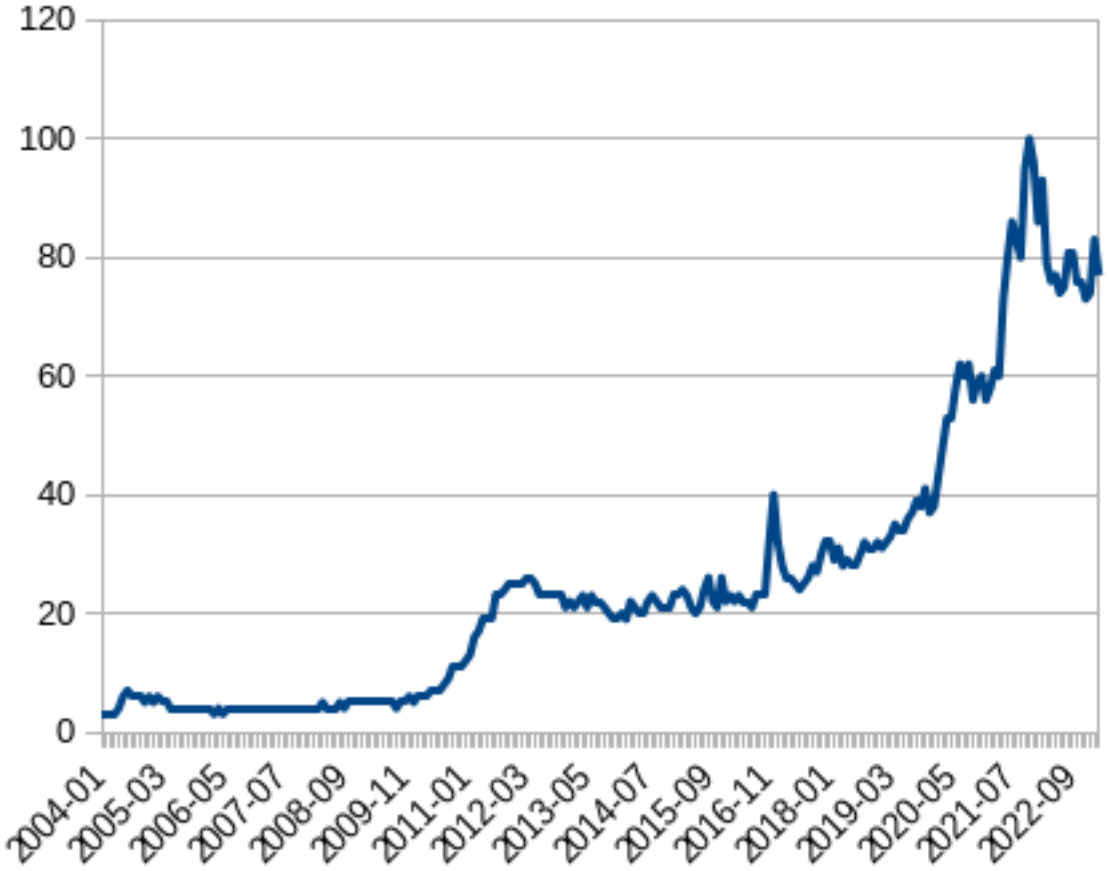
30.-31. Januar 2024, Grand Elysée Hotel Hamburg

Motivation


COVID
19
SEAFOOD

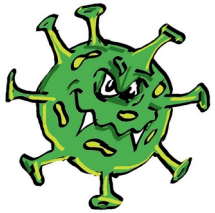

COVID CERTIFICATE
VACCINATION
JOHN
SMITH

Motivation



Thema “QR-Code” laut Google Trends

Motivation



Motivation

HP Wolf Security Threat Insights Report Q4 2022

“Threat actors are experimenting with QR codes in their lures to steal credit and debit card details from victims, for example, masquerading as parcel delivery companies seeking payment. In this type of attack, targets are more likely to access malicious websites from their mobile phones, which may lack protection against phishing.”

Motivation

HP Ireland: Maliziöse Nutzung von QR-Codes:

- Word Dokumente in Chinesisch, die behaupten, der Leser hätte Anspruch auf staatlichen Zuschuss
- Phishing-Kampagnen in Englisch, die sich als zahlungssuchende Paketzusteller ausgeben

Motivation

Smartphones:

- Meist schlechtere IT-Sicherheit
- Weniger Maßnahmen (vorhanden/installiert) als auf PCs

Letzte Studien vor der COVID-19 Pandemie

→ Wie hat sich die Situation seitdem geändert?

Stand von Forschung und Technik

- Franz et al. [7]:
  - Überblick über nutzerorientierte Phishing-Eingriffe
  - Mögliche zukünftige Forschungsrichtungen
  - Wenig Publikationen zu QR-Code-Phishing
- Einflussfaktoren auf Phishing-Angriffe
- Schädliche QR-Codes
- Zwischenfazit

Einflussfaktoren auf Phishing-Angriffe

- Cialdini [2], Gragg [10] und Stajano et al. [28]: Psychologische Faktoren
- Ferreira et al. [6]: Überblick über diese Faktoren für Social Engineering und insbesondere Phishing
- Phishing-Studien
  - z.B. Downs et al. [5], Sheng et al. [26] und Kumaraguru et al. [19]
  - Untersuchung von Faktoren wie Alter, Geschlecht und Technik-Affinität

Schädliche QR-Codes

- Kharraz et al. [13] und Lerner et al. [20]:
  - Studie zu üblichen Formen von QR-Code-Phishing
  - Häufig: Spoofing einer Passwort-geschützten Website
- Kieseberg et al. [15]: Maliziöse Pixel in QR-Codes
- Zhou et al. [33]: Invisible QR-Code Hijacking
- Dabrowski et al. [3]: Barcode-in-Barcode-Attack
- Krombholz et al. [16, 17] und Yong et al. [32]: Überblick über mögliche Angriffe und Gegenmaßnahmen

QR Code Phishing-Studien

- Mavroeidis and Nicho [22]: QR-Codes auf Fake-Google-Website
- Vidas et al. [29]: QR-Codes auf Flyer
- Sharevski et al. [25]: QR-Codes auf Website mit Login-Optionen
- Dabrowski et al. [3]: Barcode-in-Barcode-Attack
- Kumar et al. [18]: Umfrage

Zwischenfazit

- Obwohl Ansätze verschiedene Aspekte des QR-Code-Phishing untersuchten, fanden die Studien größtenteils vor der COVID-19-Pandemie statt.
- Um die Ergebnisse von früher und heute sowie an verschiedenen Standorten zu kontrollieren und zu vergleichen, ist eine neue Studie erforderlich.

Methodik

- Studie
- Umfrage

Methodik: Studie

- Angelehnt an Vidas et al. [29]: QR-Codes auf Poster
- 10 Orte am Forschungscampus Garching
  - Tendenziell Technik-versierte Teilnehmer
  - Tendenziell über 18 Jahre alt
- Zwei Arten von Postern
  - (1) einfach und (2) ansprechend gestaltet
  - Jeweils für 7 Tage ausgehängt
- Website Study-Research (SR)

Your opinion matters!

Scan Me!

Survey about the inflation in Germany

SR | Study-Research

Survey about the inflation in Germany

Help us to evaluate the impact of inflation on personal life and education. Therefore, we are looking for students and academics.

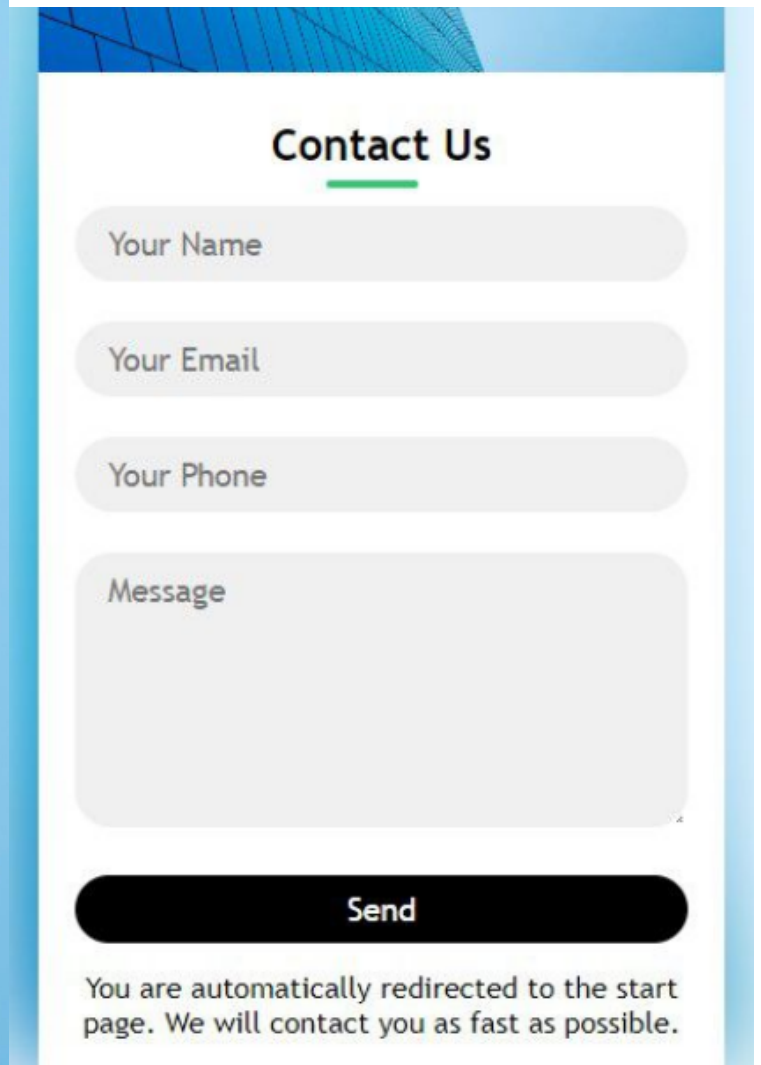
We need YOU!

Win 1/15 Amazon gift cards worth 100€

SCAN & WIN

SR

SR | Study- Research



Methodik: Umfrage

- Fragen zu
  - Beiden Postern
  - QR-Codes und Phishing allgemein
- Teilnehmende
  - Im Umfeld mit Versuch, die Teilnehmenden passend zu den Teilnehmenden der Studie zu wählen
  - Nicht am Forschungscampus möglich gewesen, wegen organisatorischer Probleme

Ergebnisse

- Studie
- Umfrage

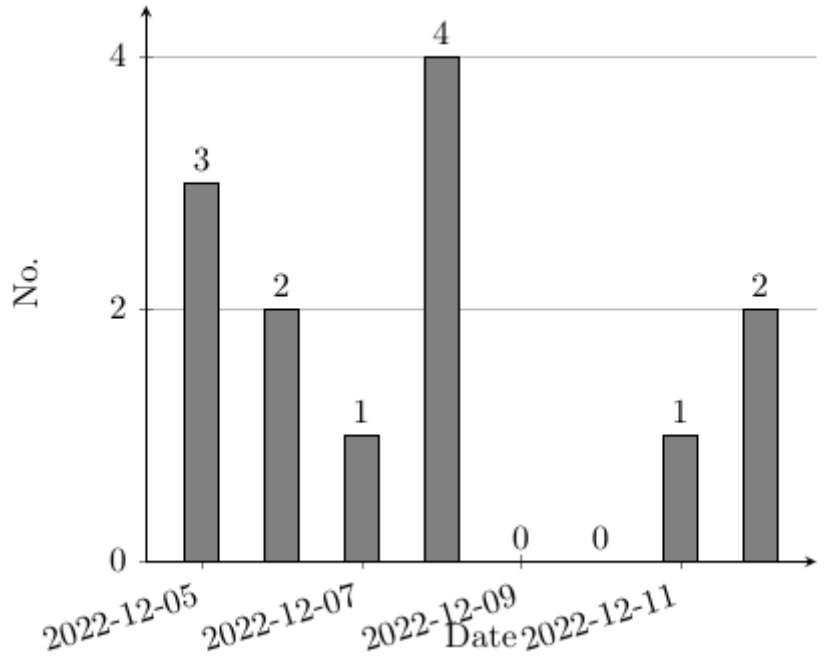
Ergebnisse: Studie

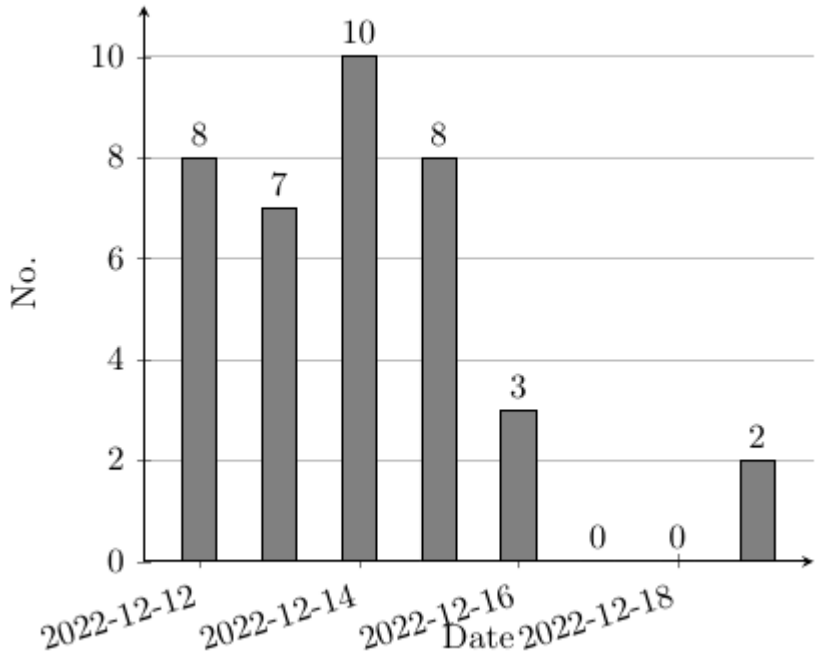
- Varianten
  - Variante 1: einfach
  - Variante 2: ansprechend

Variant	Scans	Survey	Email	Multiple
Variant 1	13 (12)	8 (7)	6 (5)	1
Variant 2	38 (25)	39 (25)	39 (25)	7
Sum	51 (37)	47 (32)	45 (30)	8

- (x): eindeutige Teilnahme
- Potenzielle Teilnehmer: 7.500 Angestellte and 17.500 Studierende

Ergebnisse: Studie (Poster 1 und 2)





Ergebnisse: Umfrage

- Teilnehmende
  - Anzahl: 123
  - Durchschnittsalter: 30,3 Jahre (Minimum: 18, Maximum: 60)
  - Geschlecht: 58 (47,16%) weiblich, 64 (52,03%) männlich und 1 (0,81%) divers
  - Beschäftigung: 33,33% Studenten, 60,98% abgeschlossenes Studium

Ergebnisse: Umfrage

- Varianten-Präferenz
  - Variante 1: 37 Teilnehmende (30,08%)
  - Variante 2: 55 Teilnehmende (44,71%)
  - Keine Variante, weil kein QR-Code gescannt wird: 31 Teilnehmende (25,20%)

Poster	No	Percentage
Variant 1	37	30.08%
Variant 2	55	44.71%
None	31	25.20%

Ergebnisse: Umfrage

- Varianten-Präferenz
  - Gründe hierfür, vgl. Tabelle

Reason	Variant 1		Variant 2	
	No.	Percentage	No.	Percentage
Professionalism	9	24.32%	24	43.64%
Trustworthy	18	48.65%	16	29.10%
Interest	4	10.81%	6	10.91%
Size and design	18	48.65%	21	38.18%
Attractiveness	4	10.81%		
Others	1	2.7%	4	34.54%
Voucher			26	47.27%
Topic			19	34.54%

Ergebnisse: Umfrage

- Interaktion mit QR-Codes

Reason	Percentage	Situation	Percentage
Functionality	70.73	COVID-19 tests	65.85
Curiosity	26.02	Restaurant visit	63.41
		University environment	34.15
Not scanning at all	13.01	Public facilities	32.52

Ergebnisse: Umfrage

- Erfahrung mit Phishing

Variant	No.	Percentage
No	39	31.71%
Email	78	63.41%
Phone (Vishing)	36	29.27%
SMS (SMiShing)	32	26.02%
Social Media	37	30.01%
Others	0	-

Diskussion

- Im Gegensatz zu Vidas et al. [29] deutlich weniger Teilnehmende
- Hierfür kann es mehrere Gründe geben: Technikaffinität, schlecht gewählter Zeitraum, bessere Awareness,…
- Für zukünftige Arbeiten URLs je nach Ort unterscheiden
- Umfrage diskutabel, da nicht die Teilnehmer der Studie teilnahmen

Fazit

- QR-Codes werden häufiger genutzt → Risiko?
  - Letzten Studien vor der Pandemie, daher Studie und Umfrage
  - Bei Studie verhältnismäßig wenig Teilnehmer
  - Umfrage zeigte Gründe für Wahl einer Variante
- Zukünftige Arbeiten
  - QR-Codes in E-Mails
  - Größere Studie mit mehr Postern

Daniela Pöhn
Forschungsinstitut CODE
Universität der Bundeswehr München

daniela.poehn@unibw.de
https://www.unibw.de/code