What is Phishing?

- **Phishing** is when a scammer uses fraudulent emails or texts, or copycat websites to get you to share valuable personal information
  - Account numbers
  - Social Security numbers
  - Account login IDs and passwords
- Scammers use your information to steal your money or your identity or both.

pcgit Advanced IT Support

https://www.consumer.ftc.gov/articles/0003-phishing

The Brutal Reality of Data Breaches

Target:

70 million records stolen
46% ⬇ in profit
Cost: **$162 million**

RSA Security:

40 million employee records stolen.
Cost: **$66 million**

Sony Playstation:

77 million accounts hacked
Offline for 23 days
Cost: **$177 million**

Small Businesses are hit every day:

Dental practice **$33,000**

Restaurant: **$99,000**

Bowling alley: **$60,000**

MyGlue

Phishing is a Cyber Attack

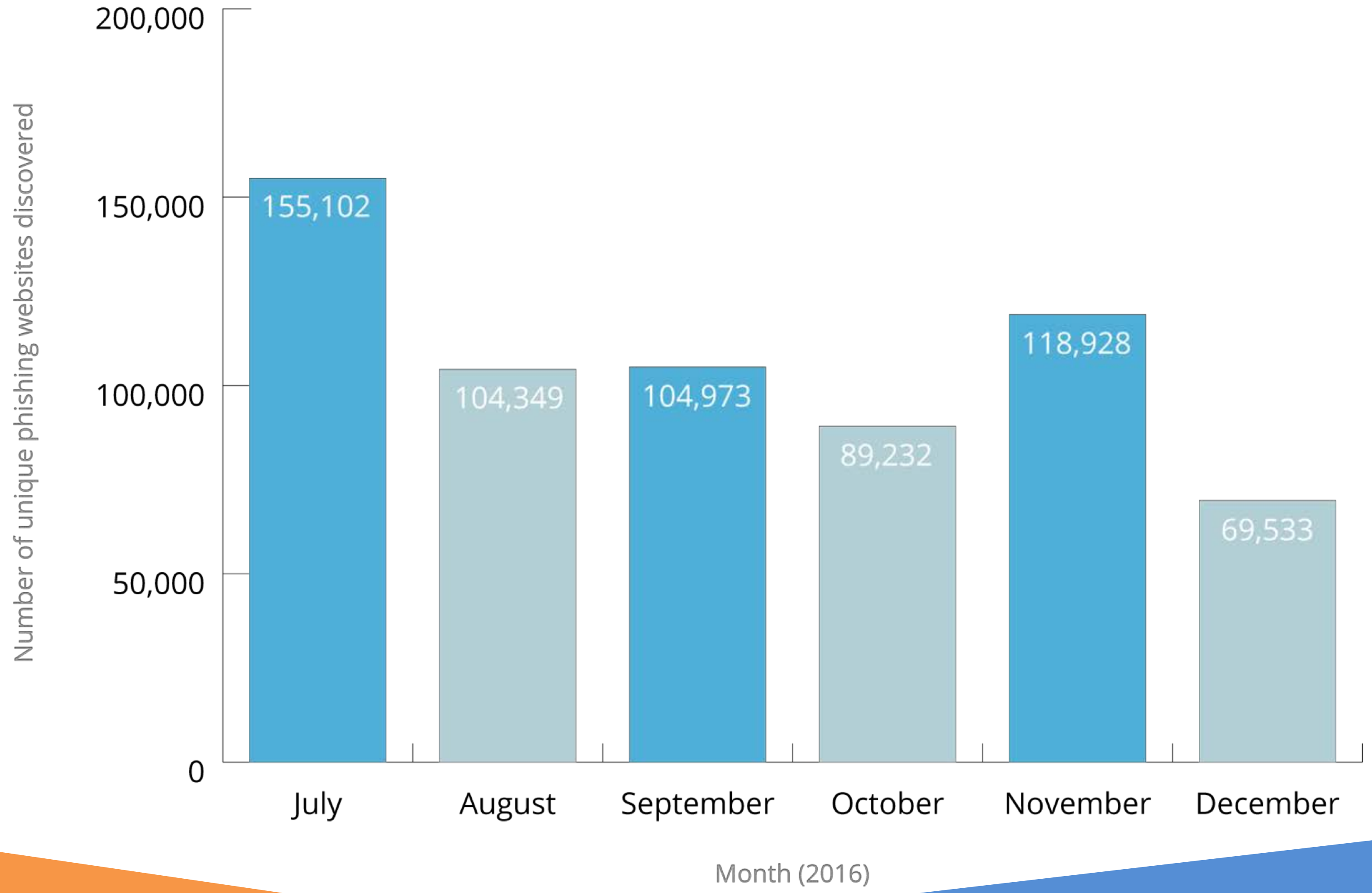
- According to the National Cyber Security Alliance, 60% of small and midsized businesses that are hacked go out of business within six months.
- 62% out of 1,377 CEO respondents said that their firms don't have an up-to-date or active cybersecurity strategy--or any strategy at all.

pcgit Advanced IT Support

https://www.inc.com/joe-galvin/60-percent-of-small-businesses-fold-within-6-months-of-a-cyber-attack-heres-how-to-protect-yourself.html

Cybercriminals Are Phishing for Sensitive Business Information

With phishing attacks steadily on the rise, businesses have to be especially careful when clicking links or opening email messages from untrusted sources. The chart below shows the number of unique phishing websites detected monthly in the last two quarters of 2016.

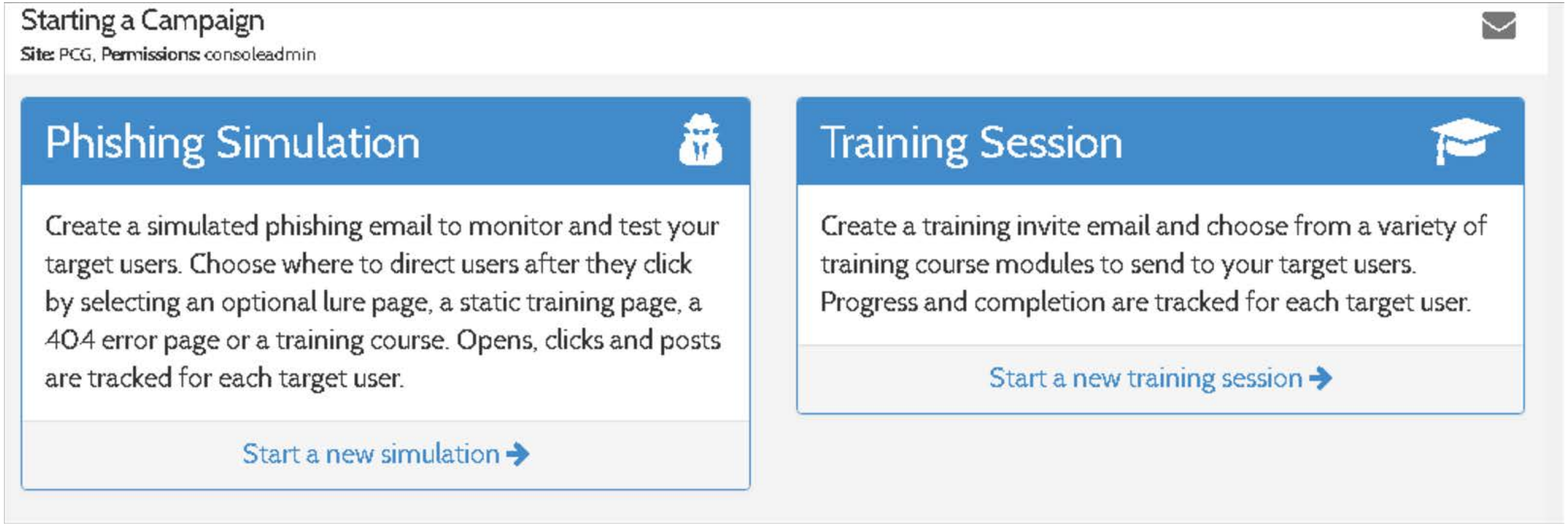


APWG, *"Phishing Activity Trends Report"* 4th Quarter, 2016

How to Avoid being Phished

- Users are the weakest link in the security chain.
- Train your users
  - Education
  - Testing

Phishing Avoidance Training



Starting a Campaign

Site: PCG, **Permissions:** consoleadmin

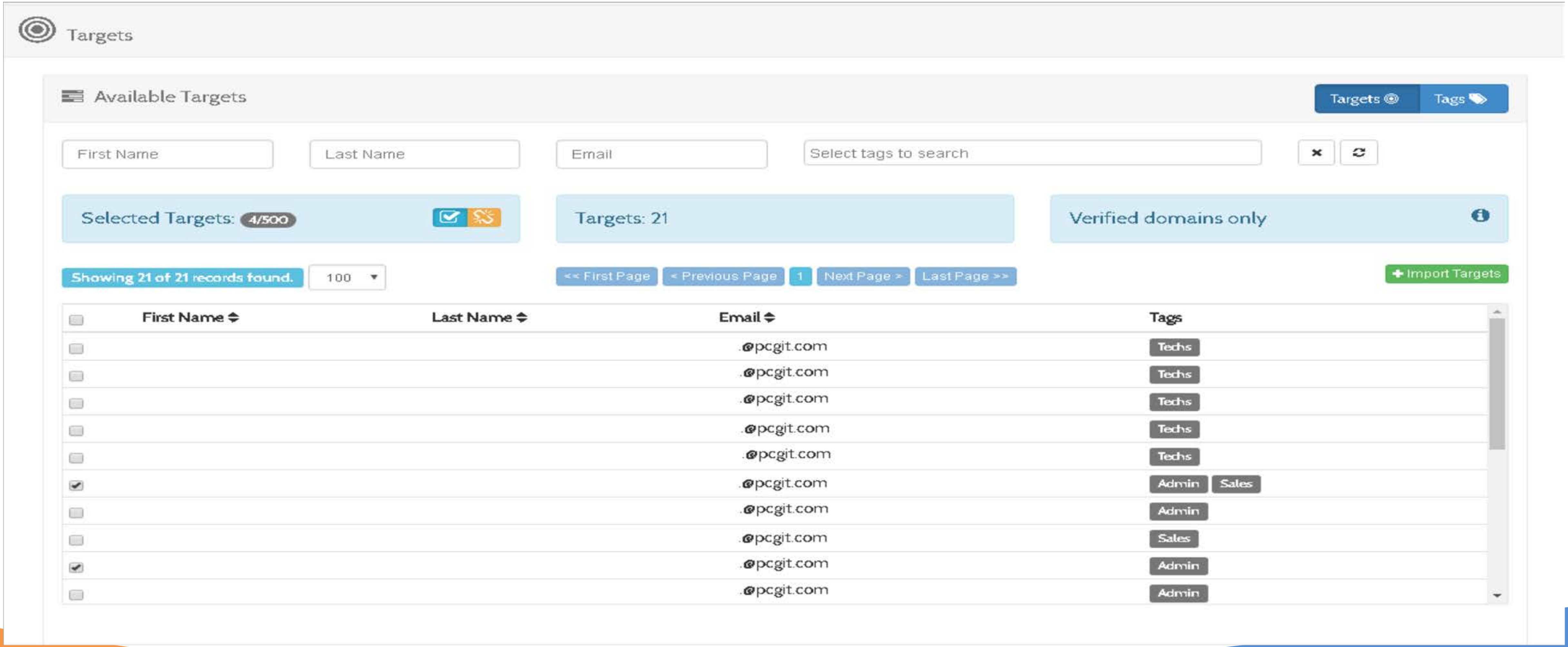
Phishing Simulation

Create a simulated phishing email to monitor and test your target users. Choose where to direct users after they click by selecting an optional lure page, a static training page, a 404 error page or a training course. Opens, clicks and posts are tracked for each target user.

Training Session

Create a training invite email and choose from a variety of training course modules to send to your target users. Progress and completion are tracked for each target user.

Phishing Avoidance Training



Selected Targets: 4/500

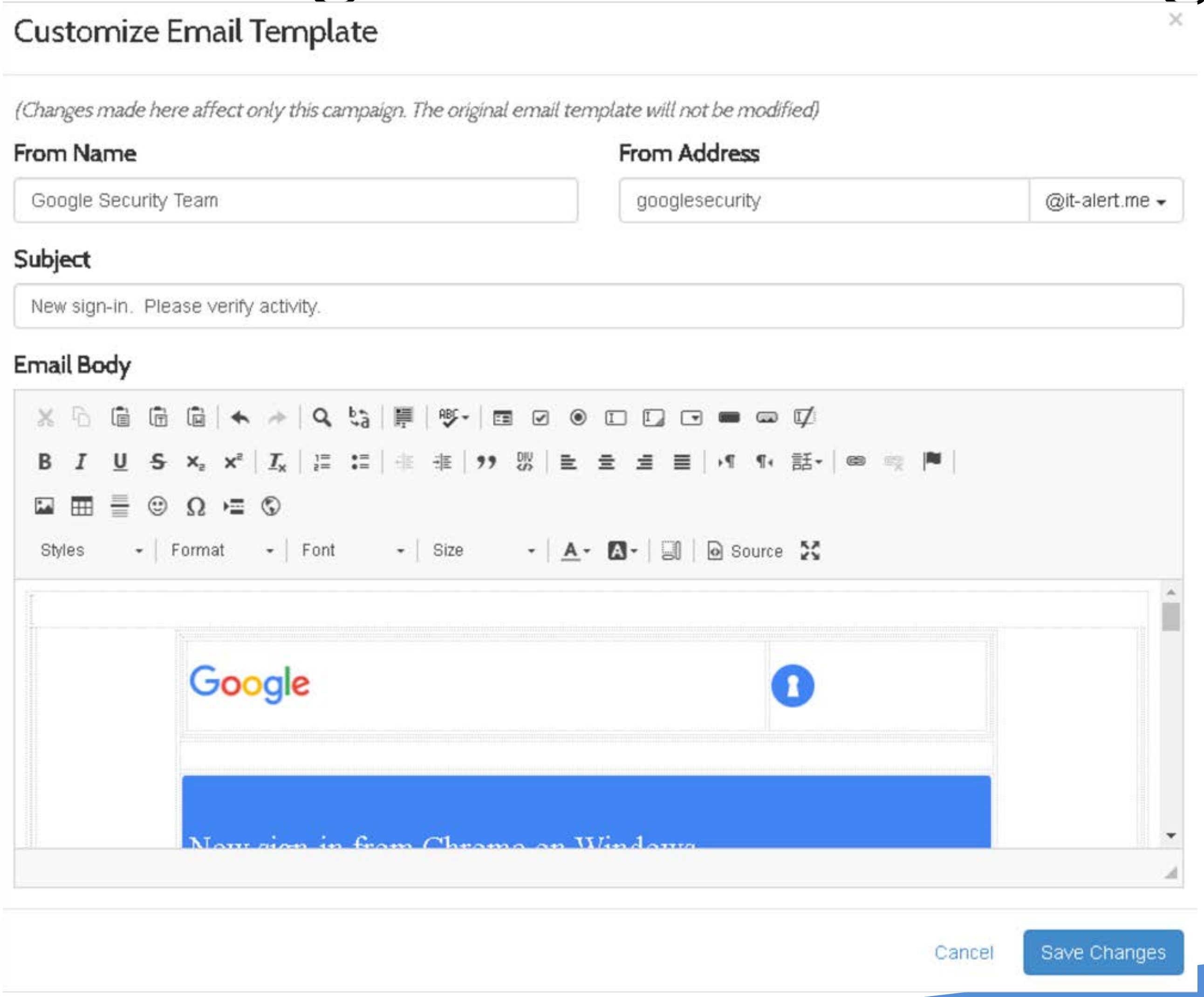
Targets: 21

Verified domains only

Showing 21 of 21 records found. 100

□	First Name	Last Name	Email	Tags
□			.@pcgit.com	Techs
□			.@pcgit.com	Techs
□			.@pcgit.com	Techs
□			.@pcgit.com	Techs
□			.@pcgit.com	Techs
☑			.@pcgit.com	Admin Sales
□			.@pcgit.com	Admin
□			.@pcgit.com	Sales
☑			.@pcgit.com	Admin
□			.@pcgit.com	Admin

Phishing Avoidance Training



Customize Email Template

(Changes made here affect only this campaign. The original email template will not be modified)

From Name: Google Security Team

From Address: googlesecurity @it-alert.me

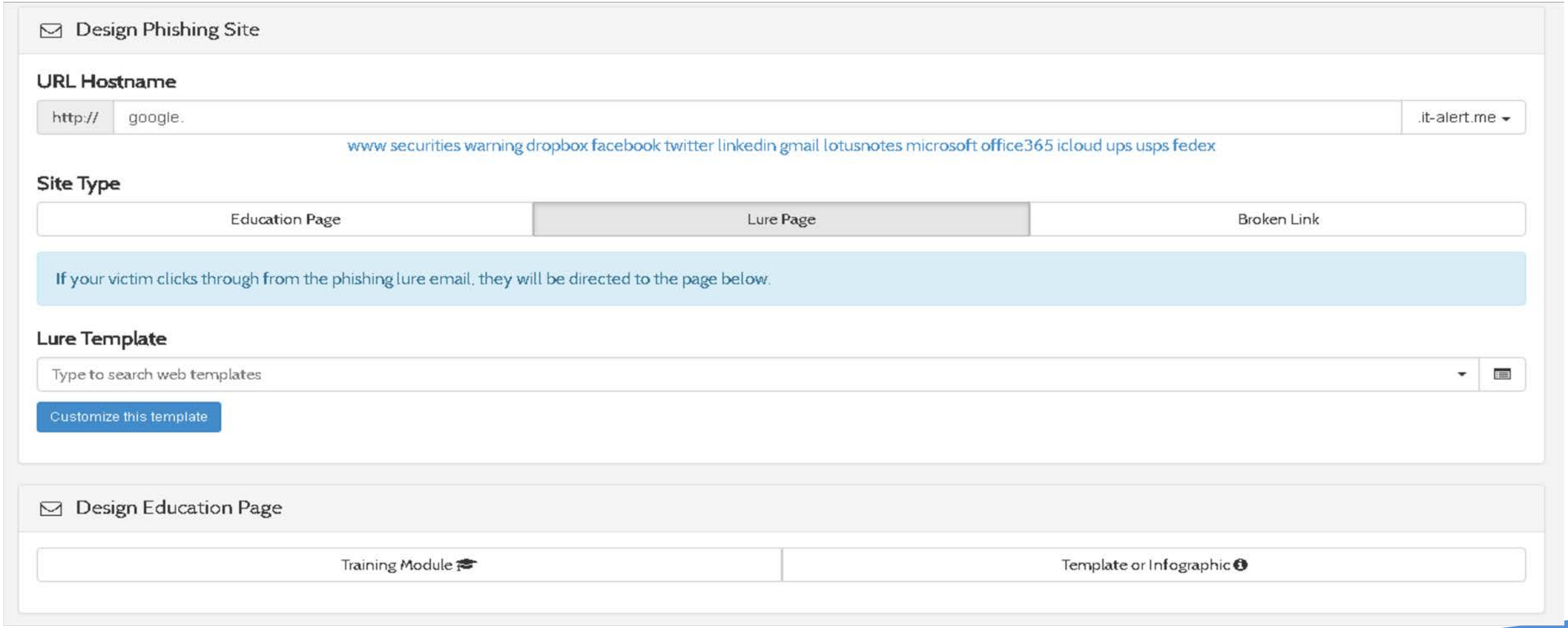
Subject: New sign-in. Please verify activity.

Email Body

New sign-in from Chrome on Windows

pcgit Advanced IT Support

Phishing Avoidance Training



Design Phishing Site

URL Hostname

http:// google. .it-alert.me

www securities warning dropbox facebook twitter linkedin gmail lotusnotes microsoft office365 icloud ups usps fedex

Site Type

Education Page | Lure Page | Broken Link

If your victim clicks through from the phishing lure email, they will be directed to the page below.

Lure Template

Type to search web templates

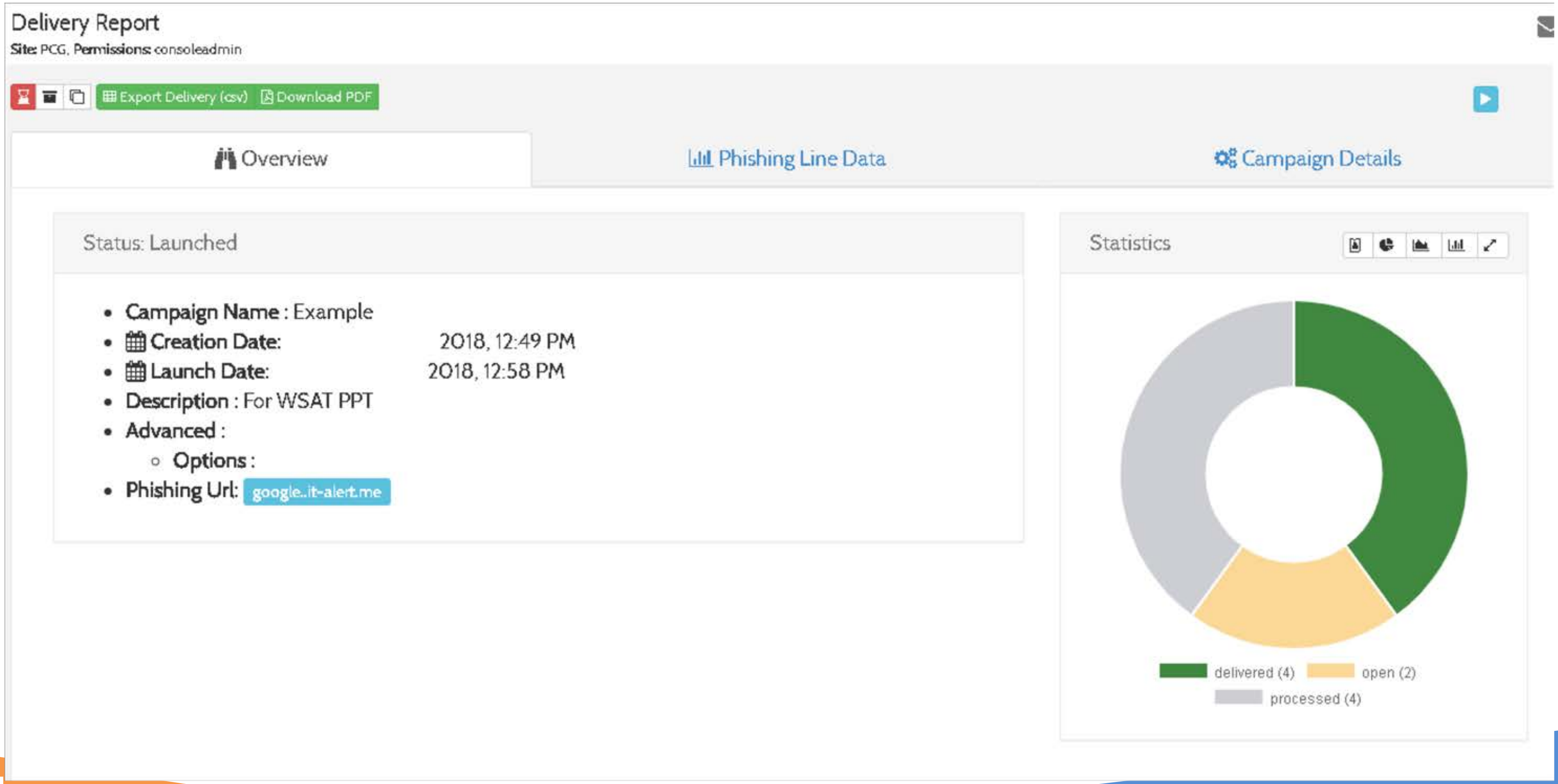
Customize this template

Design Education Page

Training Module | Template or Infographic

pcgit Advanced IT Support

Phishing Avoidance Training



Delivery Report

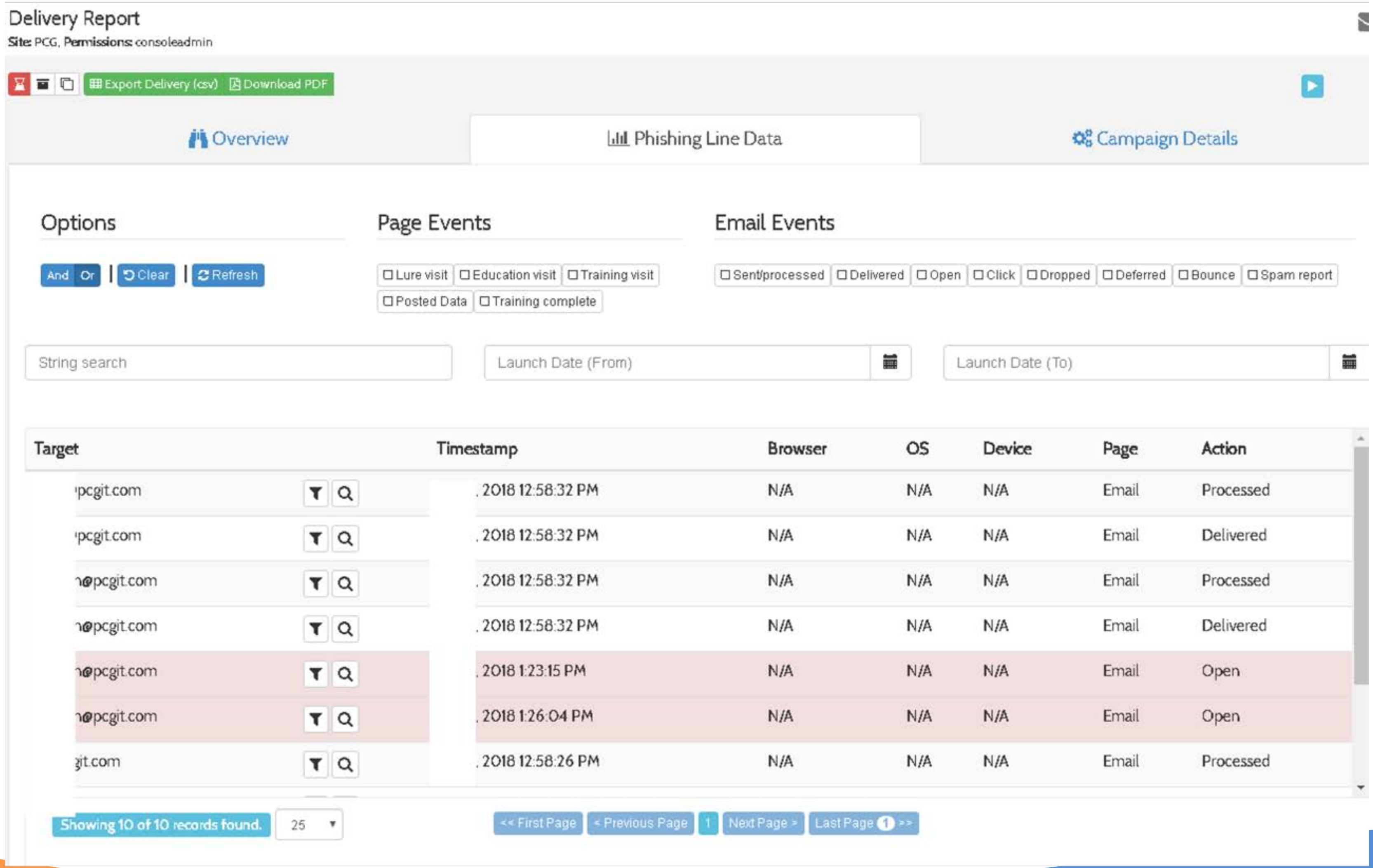
Site: PCG, **Permissions:** consoleadmin

Status: Launched

- **Campaign Name** : Example
- **Creation Date:** 2018, 12:49 PM
- **Launch Date:** 2018, 12:58 PM
- **Description** : For WSAT PPT
- **Advanced** :
  - **Options** :
- **Phishing Url:** google..it-alert.me

Statistics

Phishing Avoidance Training



Delivery Report

Site: PCG, **Permissions:** consoleadmin

Options

Page Events

☐ Lure visit ☐ Education visit ☐ Training visit ☐ Posted Data ☐ Training complete

Email Events

☐ Sent/processed ☐ Delivered ☐ Open ☐ Click ☐ Dropped ☐ Deferred ☐ Bounce ☐ Spam report

Target	Timestamp	Browser	OS	Device	Page	Action
'pcgit.com	, 2018 12:58:32 PM	N/A	N/A	N/A	Email	Processed
'pcgit.com	, 2018 12:58:32 PM	N/A	N/A	N/A	Email	Delivered
n@pcgit.com	, 2018 12:58:32 PM	N/A	N/A	N/A	Email	Processed
n@pcgit.com	, 2018 12:58:32 PM	N/A	N/A	N/A	Email	Delivered
n@pcgit.com	, 2018 1:23:15 PM	N/A	N/A	N/A	Email	Open
n@pcgit.com	, 2018 1:26:04 PM	N/A	N/A	N/A	Email	Open
git.com	, 2018 12:58:26 PM	N/A	N/A	N/A	Email	Processed

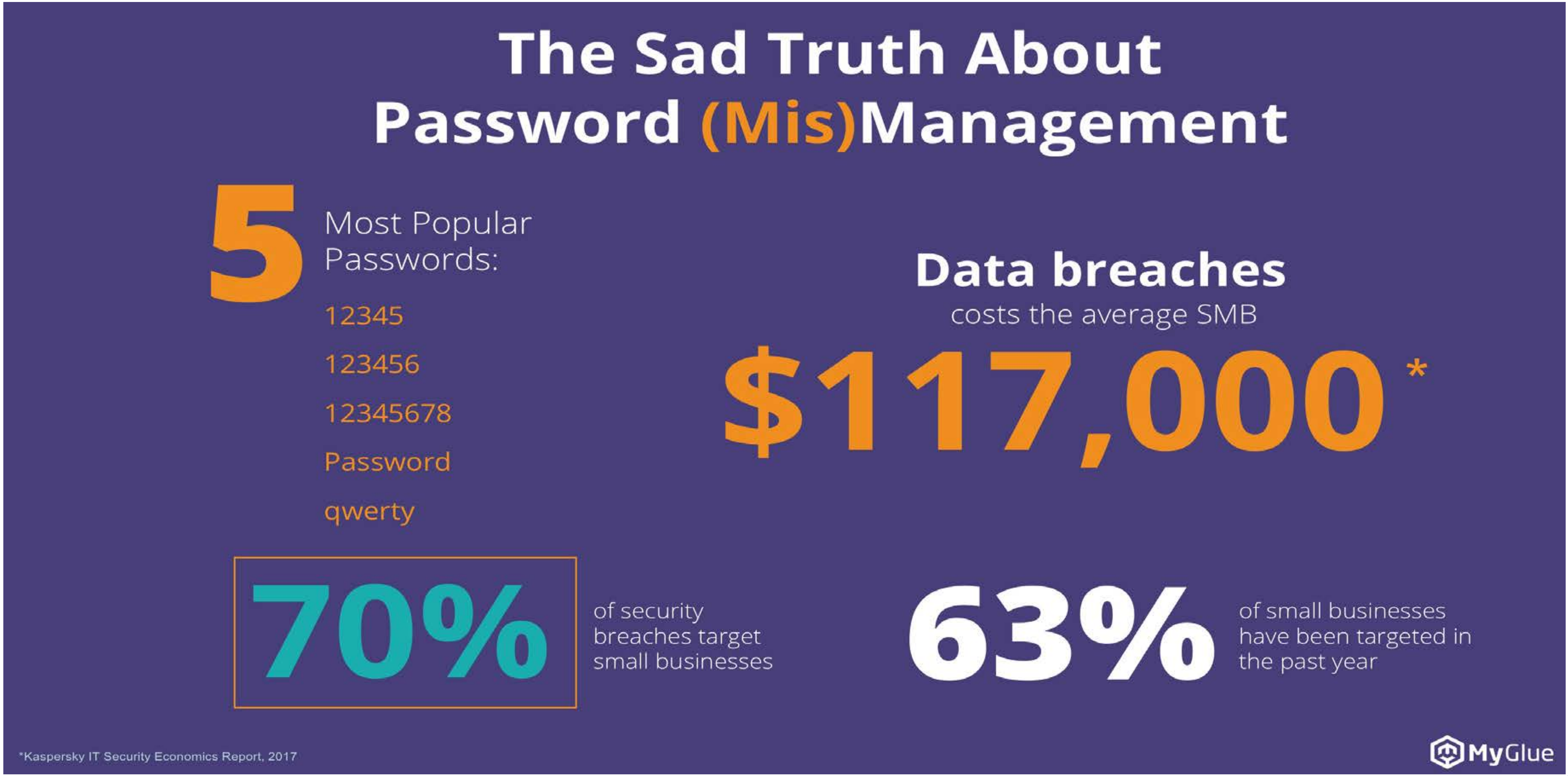
Showing 10 of 10 records found. 25

pcgit
Advanced IT Support

Password Security

- The average business employee must keep track of **191** passwords
- **81%** of confirmed data breaches are due to passwords.
- The average 250-employee company has **47,750** passwords in use
- **61%** of people use the same or a similar password everywhere, despite knowing that it's not a secure practice.
- The average employee types out credentials to authenticate to their websites and apps **154** times per month. They also share about four passwords with others.

https://www.securitymagazine.com/articles/88475-average-business-user-has-191-passwords



The Sad Truth About Password (Mis)Management

5 Most Popular Passwords:

12345

123456

12345678

Password

qwerty

Data breaches costs the average SMB

$117,000 *

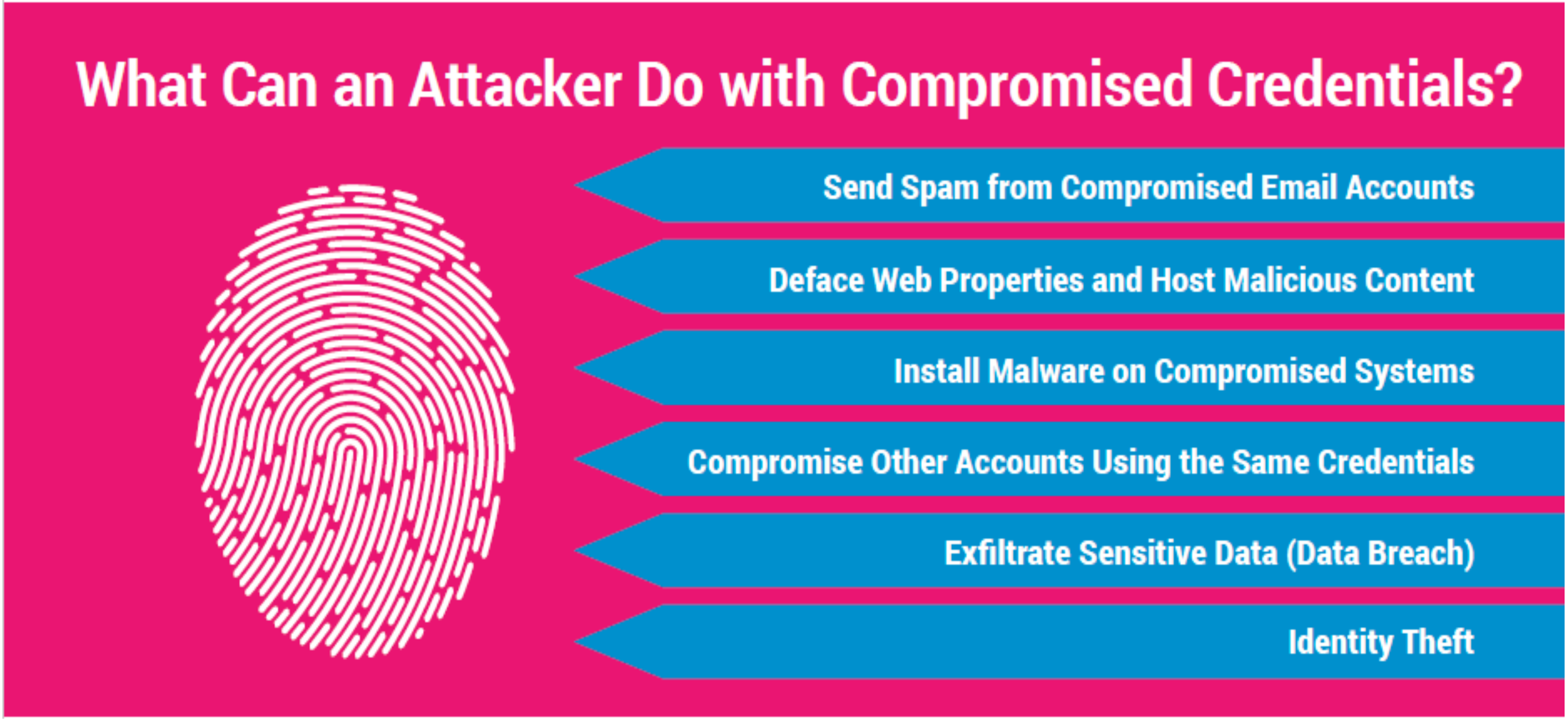
70% of security breaches target small businesses

63% of small businesses have been targeted in the past year

*Kaspersky IT Security Economics Report, 2017

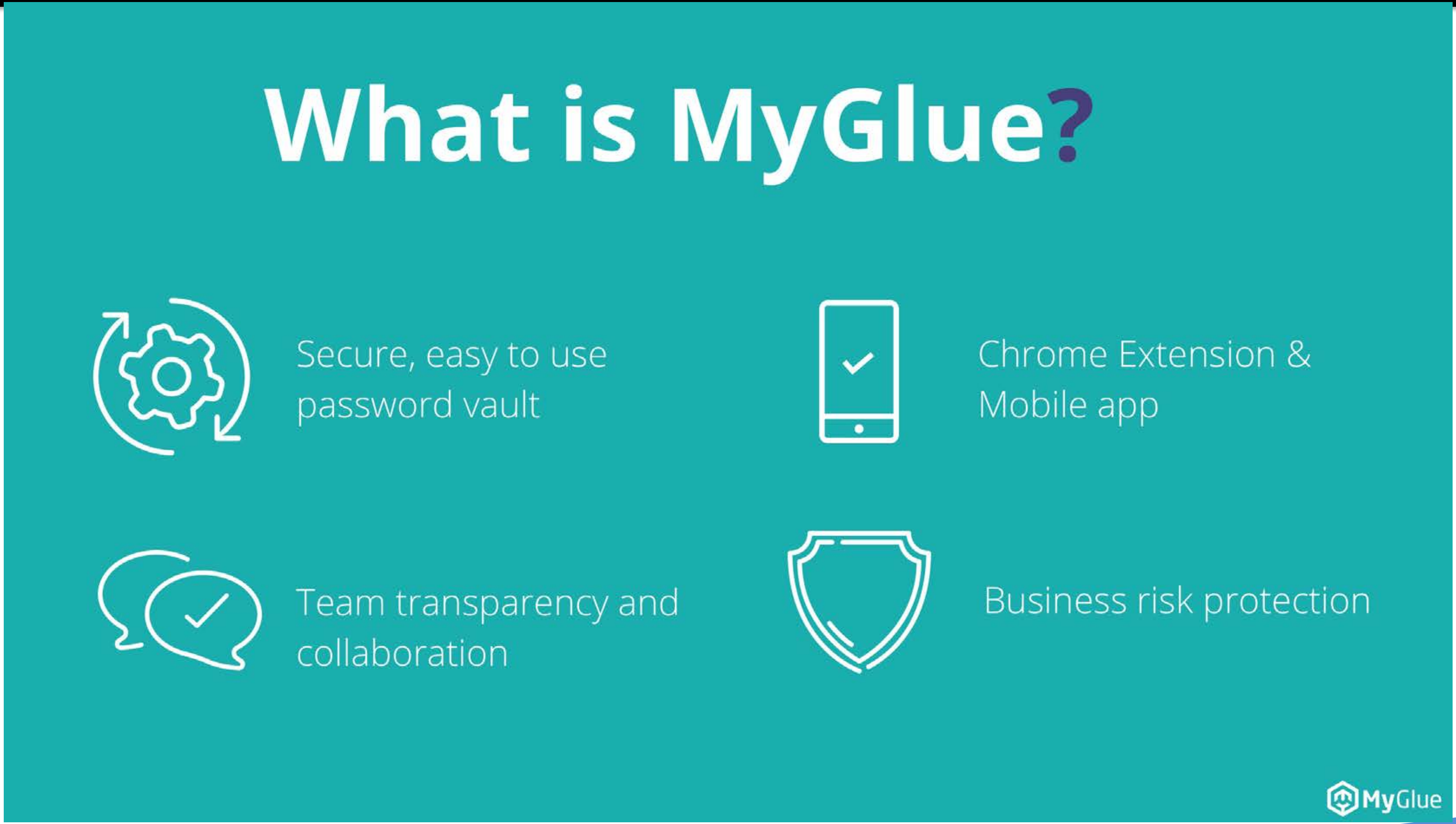
MyGlue

*Kaspersky IT Security Economics Report, 2017



What Can an Attacker Do with Compromised Credentials?

- Send Spam from Compromised Email Accounts
- Deface Web Properties and Host Malicious Content
- Install Malware on Compromised Systems
- Compromise Other Accounts Using the Same Credentials
- Exfiltrate Sensitive Data (Data Breach)
- Identity Theft



What is MyGlue?

- Secure, easy to use password vault
- Chrome Extension & Mobile app
- Team transparency and collaboration
- Business risk protection

Multi-Factor Authentication Factors

- Something you know (password, PIN)
- Something you have (phone, RSA token, USB token)
- Something you are (fingerprint, facial recognition)
- Where you are (GPS, network address)
- Time (work schedule)

Multi-Factor Authentication – Why?

- Identity theft is the fastest-growing type of crime and is now more profitable than drug-related crimes.
- Weak or stolen user credentials are hackers' weapon of choice, used in 95 percent of all Web application attacks.
- Of all targeted attacks, 31 percent are aimed at businesses with fewer than 250 employees.

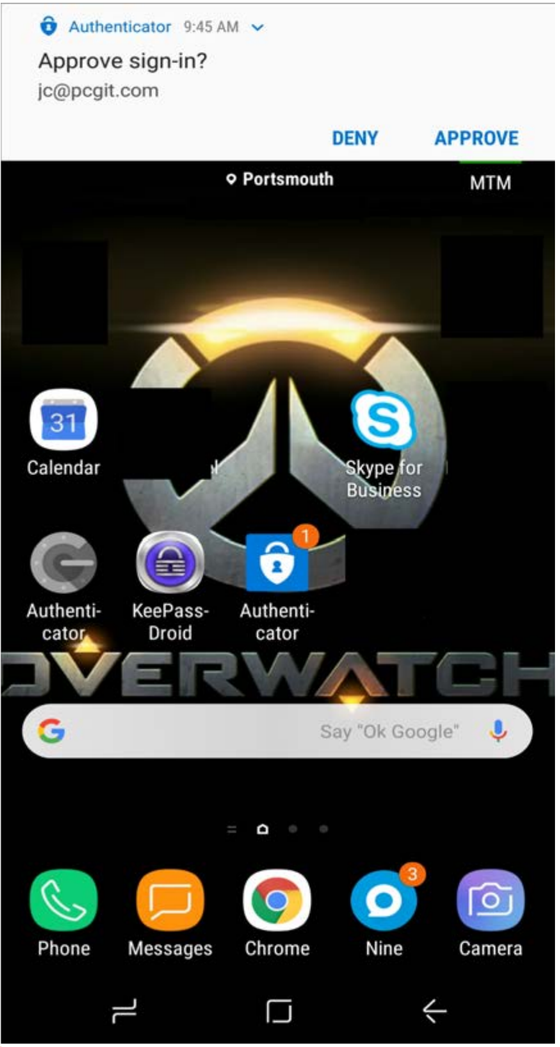
Multi-Factor Authentication – How?

- SMS – not preferred, spoofable
- Call – also not preferred, spoofable
- Code Generator app – Duo,Google Authenticator, Authy, MS Authenticator
- Push app – Duo, MS Authenticator, Google Prompt, Authy
- Hardware – Most secure. USB/NFC – YubiKey, RSA

Multi-Factor Authentication – Where?

- Wherever possible!
  - Social media (Twitter, Facebook, Instagram, LinkedIn)
  - Tools (major email providers, Apple, Microsoft)
  - Shopping (Amazon, Etsy, Venmo)
- Does a website support 2FA/MFA? - https://twofactorauth.org/

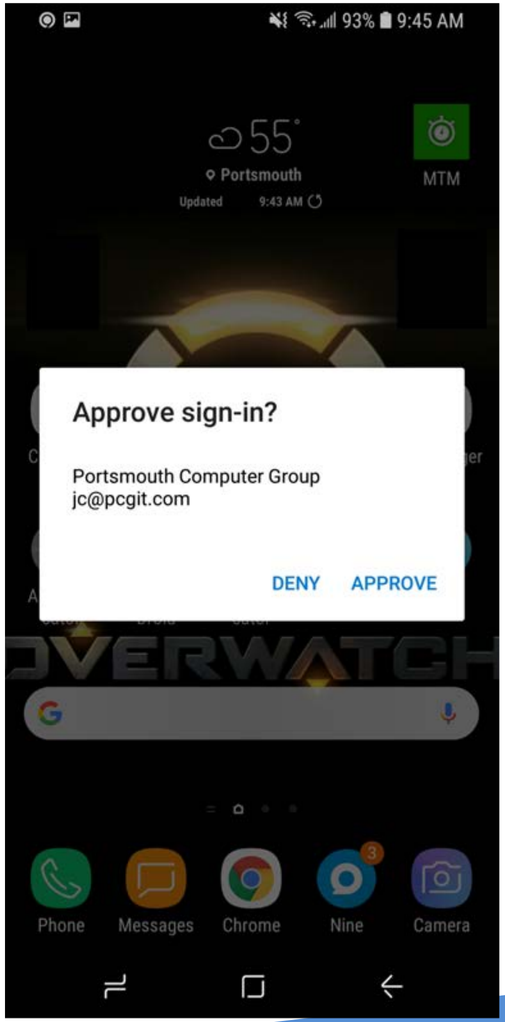
Multi-Factor Authentication – MS Push



Authenticator 9:45 AM

Approve sign-in?

jc@pcgit.com

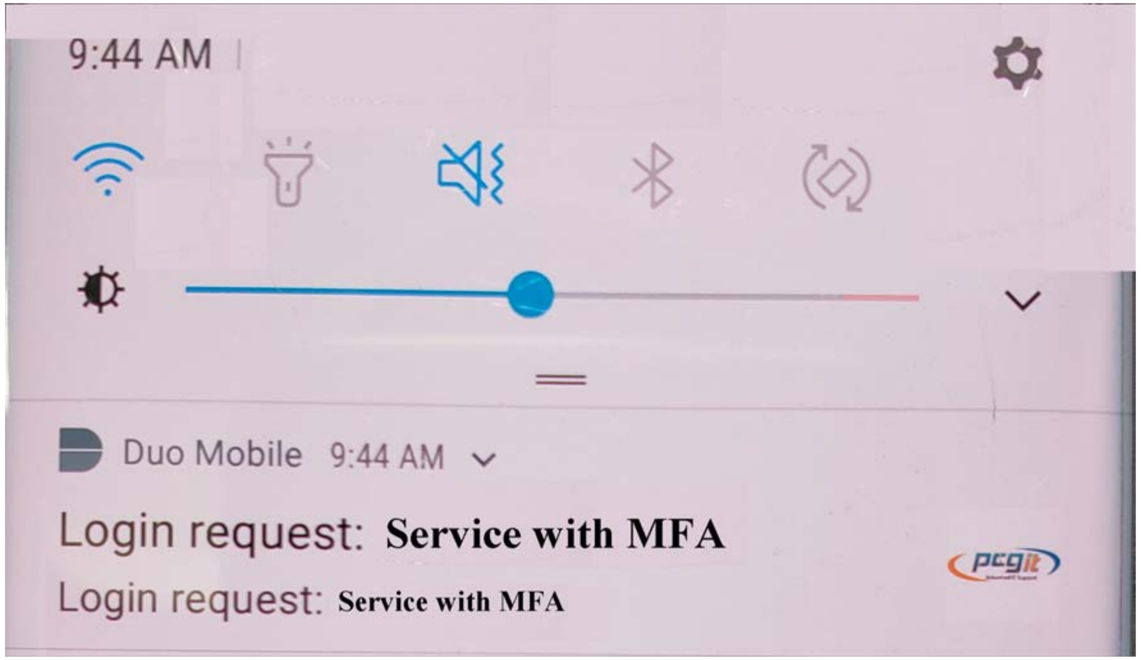


Approve sign-in?

Portsmouth Computer Group
jc@pcgit.com

pcgit Advanced IT Support

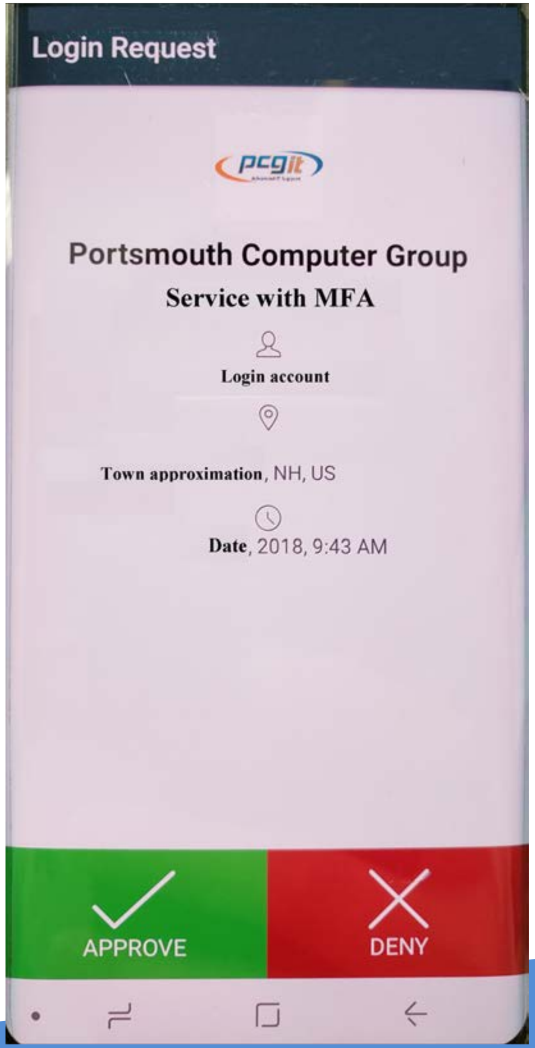
Multi-Factor Authentication – Duo Push



Duo Mobile 9:44 AM

Login request: **Service with MFA**

Login request: **Service with MFA**



Portsmouth Computer Group

Service with MFA

Login account

Town approximation, NH, US

Date, 2018, 9:43 AM