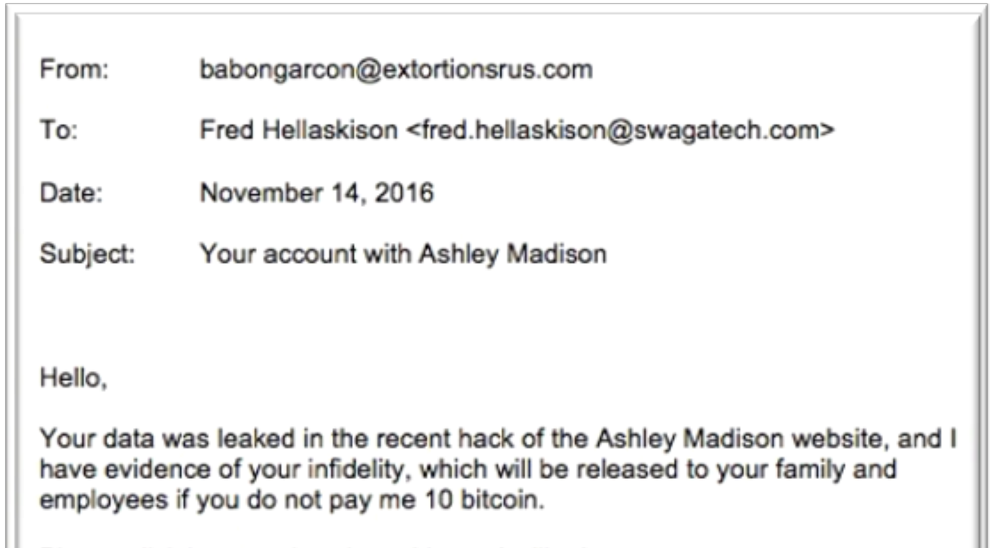
Phishing Assessment Optimizer™

Make sure you're getting value and not wasting time!



From: babongarcon@extortionsrus.com

To: Fred Hellaskison <fred.hellaskison@swagatech.com>

Date: November 14, 2016

Subject: Your account with Ashley Madison

Hello,

Your data was leaked in the recent hack of the Ashley Madison website, and I have evidence of your infidelity, which will be released to your family and employees if you do not pay me 10 bitcoin.

Please click here to view the evider

Once you have verified my evidenc paying my fee.

Thanks,

B. A. Bongarcon

WWW.CLICKARMOR.CA

Why do you need this Phishing Assessment Optimizer?

Having delivered "security awareness training" and "phishing assessments" for many years, I found that there were numerous variables and potential pitfalls that could cause adverse outcomes for an awareness program, and for the employees in an organization.

*I designed the **"Phishing Assessment Optimizer"** as a tool to help IT and Security Managers anticipate and address these pitfalls before they happen when you are using live, "mock phishing exercises".*

*If you aren't avoiding these issues, you might only have "**Security Theater**", because sometimes management just wants "click rates" no matter how they were generated. This is not helping your organization become secure.*

No organization can afford to waste time and money on bad assessments.

Scott Wright, CISA
CEO and Founder
Click Armor

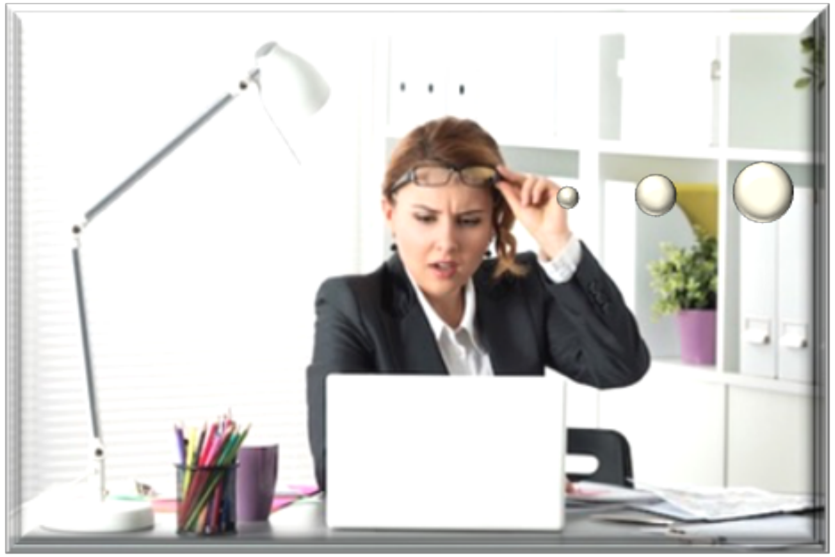
WWW.CLICKARMOR.CA

Book a Call

http://twitter.com/clickarmor

Table of Contents

Pitfall #1: Unpredictable employee actions



OMG! Wait until **Twitter** hears about this…

Do you have a plan for unexpected end-user actions?

- Unlike "**technical penetration tests**" that have "***terms of engagement***", a **"human vulnerability test"** of any kind can have unexpected results
- Discuss expected and "**potential**" results of each test message, and the **risks**, with management

Book a Call

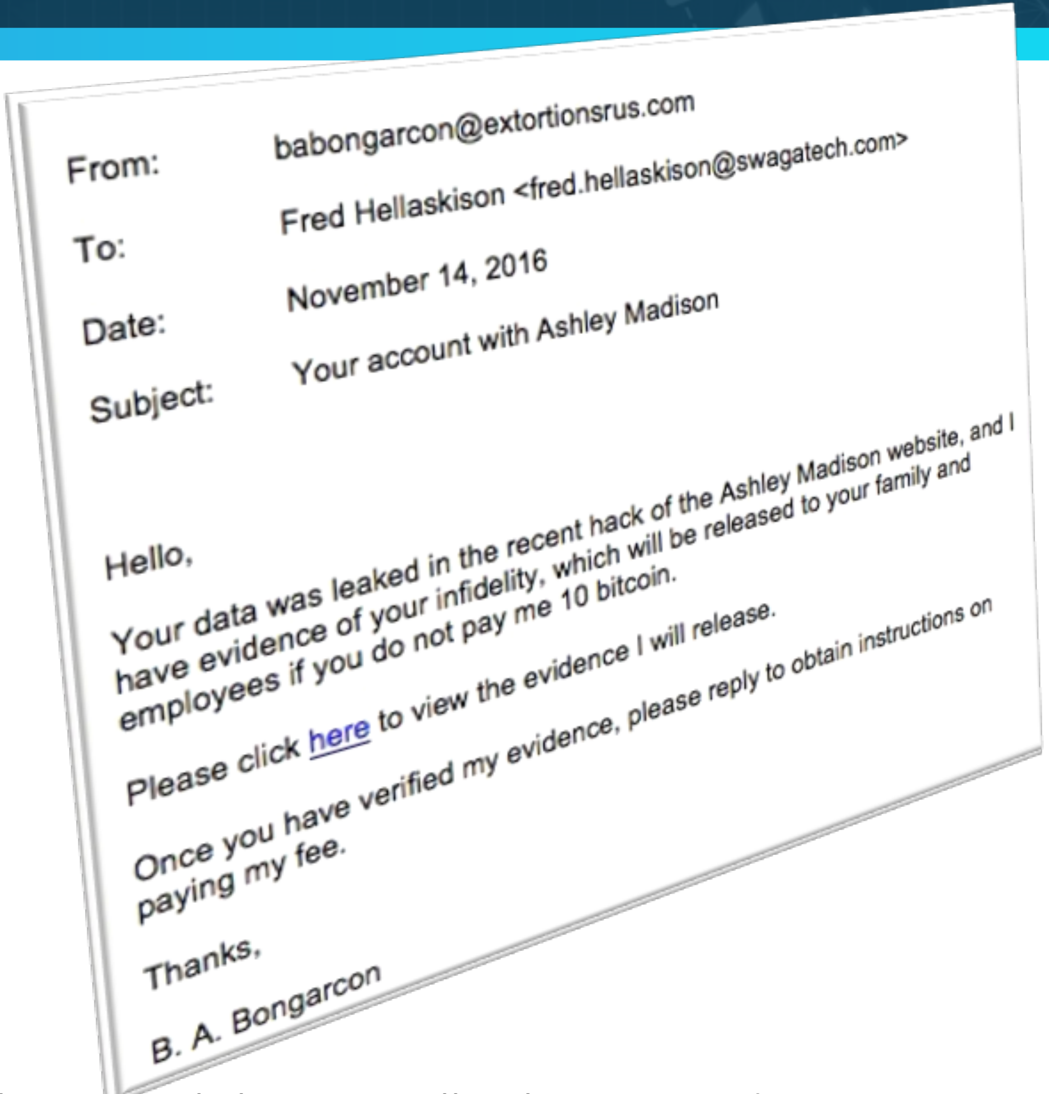
Pitfall #2: Impossibly difficult test messages

- The point is NOT to prove you're smarter than employees or shame them. This can easily backfire.
- While it's not easy, always **leave fair clues** you can point to for learning in live tests.

Are you having too much fun tricking users?

Book a Call

Pitfall #3: Embarrassing your employees - *“The boss clicked on WHAT???”*



From: babongarcon@extortionsrus.com

To: Fred Hellaskison <fred.hellaskison@swagatech.com>

Date: November 14, 2016

Subject: Your account with Ashley Madison

Hello,

Your data was leaked in the recent hack of the Ashley Madison website, and I have evidence of your infidelity, which will be released to your family and employees if you do not pay me 10 bitcoin.

Please click here to view the evidence I will release.

Once you have verified my evidence, please reply to obtain instructions on paying my fee.

Thanks,

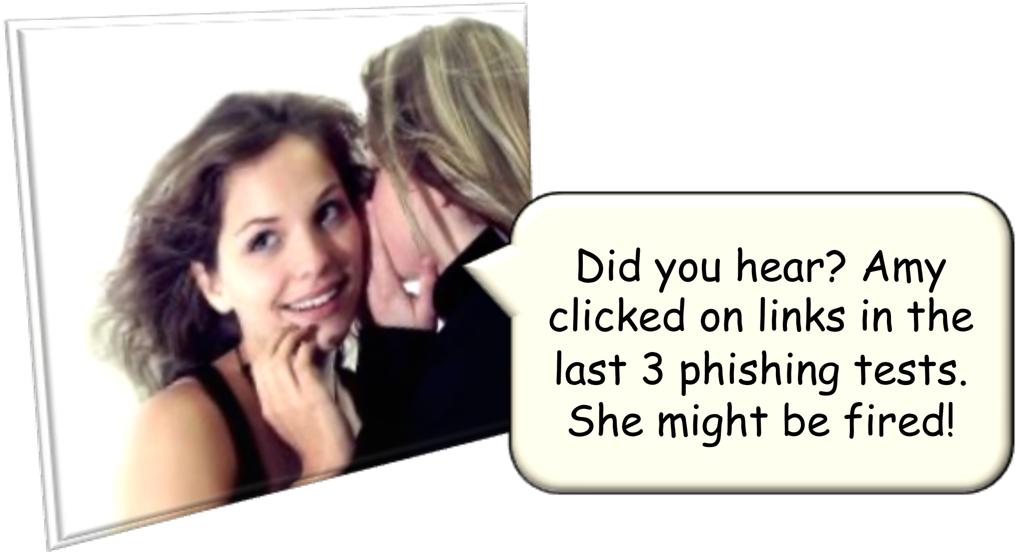
B. A. Bongarcon

- Think about the possible actions and consequences for employees
- Avoid controversial subjects that could put employees in a difficult position in live tests

Are your emails too leading?

Book a Call

Pitfall #4: Employee confidentiality risks


Did you hear? Amy clicked on links in the last 3 phishing tests. She might be fired!

- The raw data results of live phishing tests are sensitive
- Treat them as Personally Identifiable Information (PII)

Do you have access and need-to-know restrictions on results?

Pitfall #5: Employee targeting backlash

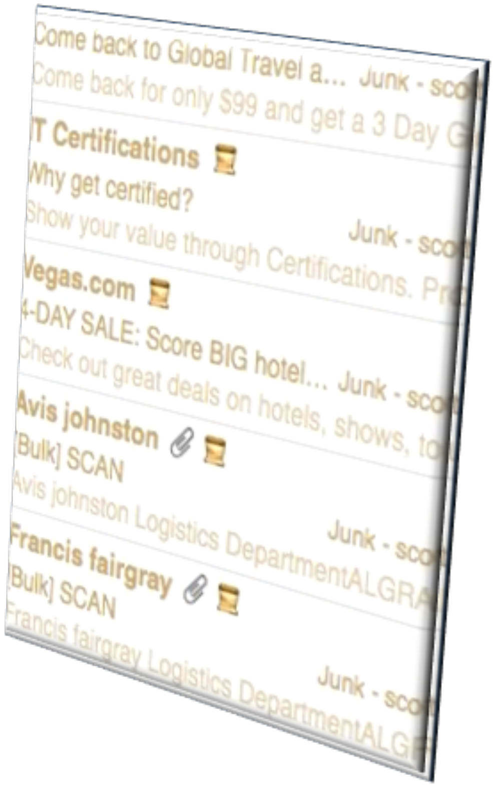
- Employees can be sensitive to unfair victimization in live tests (and may launch grievances?)
- *Get **HR and Legal** involved early (GULP!)*

Are you doing damage to the corporate culture?

Book a Call

Pitfall #6: Unpredictable spam filters and settings

- If they don’t see the message, what level of precision in results is meaningful?
- Spam traps and “image preview settings” can skew results
- White-list the email sending domain/IP’s
- Run some small live tests
- Some normalization techniques may help (but normalization that only compensates based on “open rates” can also be skewed)
- Put disclaimers on baseline and trend data regarding variables like these



Come back to Global Travel a... Junk - sco
Come back for only $99 and get a 3 Day G

T Certifications
Why get certified?
Show your value through Certifications. Pr
Junk - sco

Vegas.com
4-DAY SALE: Score BIG hotel... Junk - sco
Check out great deals on hotels, shows, to

Avis johnston
[Bulk] SCAN
Avis johnston Logistics DepartmentALGRA
Junk - sco

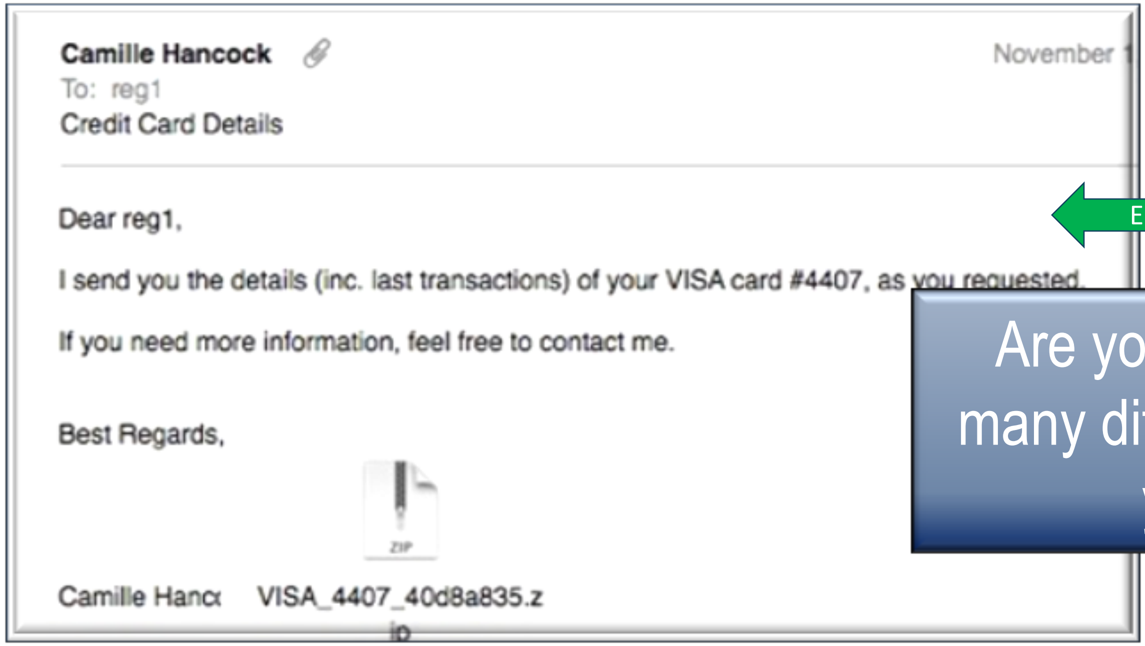
Francis fairgray
[Bulk] SCAN
Francis fairgray Logistics DepartmentALG
Junk - sco

Are your results getting skewed by filters and settings?

Book a Call

Pitfall #7: Too many variables in difficulty of test messages

- Trends can be hard to track if you vary the difficulty of live tests too much
- Management might push for more difficulty
- Keep the difficulty **consistent** for usable data



Camille Hancock November 1

To: reg1

Credit Card Details

Dear reg1,

I send you the details (inc. last transactions) of your VISA card #4407, as you requested.

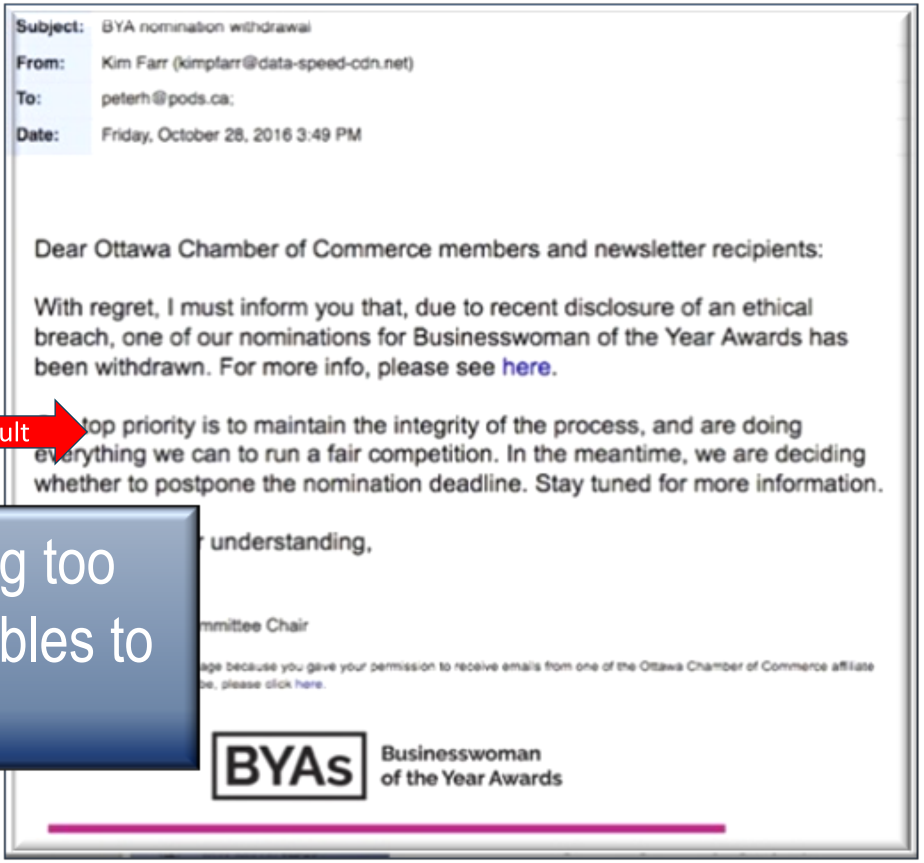
If you need more information, feel free to contact me.

Best Regards,

Camille Hanc VISA_4407_40d8a835.zip

Easy

Difficult



Subject: BYA nomination withdrawal

From: Kim Farr (kimpfarr@data-speed-cdn.net)

To: peterh@pods.ca;

Date: Friday, October 28, 2016 3:49 PM

Dear Ottawa Chamber of Commerce members and newsletter recipients:

With regret, I must inform you that, due to recent disclosure of an ethical breach, one of our nominations for Businesswoman of the Year Awards has been withdrawn. For more info, please see here.

top priority is to maintain the integrity of the process, and are doing everything we can to run a fair competition. In the meantime, we are deciding whether to postpone the nomination deadline. Stay tuned for more information.

understanding,

mmittee Chair

age because you gave your permission to receive emails from one of the Ottawa Chamber of Commerce affiliate
be, please click here.

Are you introducing too many difficulty variables to your data?

Book a Call

Pitfall #8: Forbidden "Hot Button" impersonations

- ***Hot-button impersonations*** are roles in the organization that are "*too sensitive to simulate*" in live campaigns
- Attackers can guess or learn where they are, making campaigns less effective
- Try to make them "in-scope", or else recognize that the **scope of testing can be significantly limited**

What areas can't be tested that attackers will target?

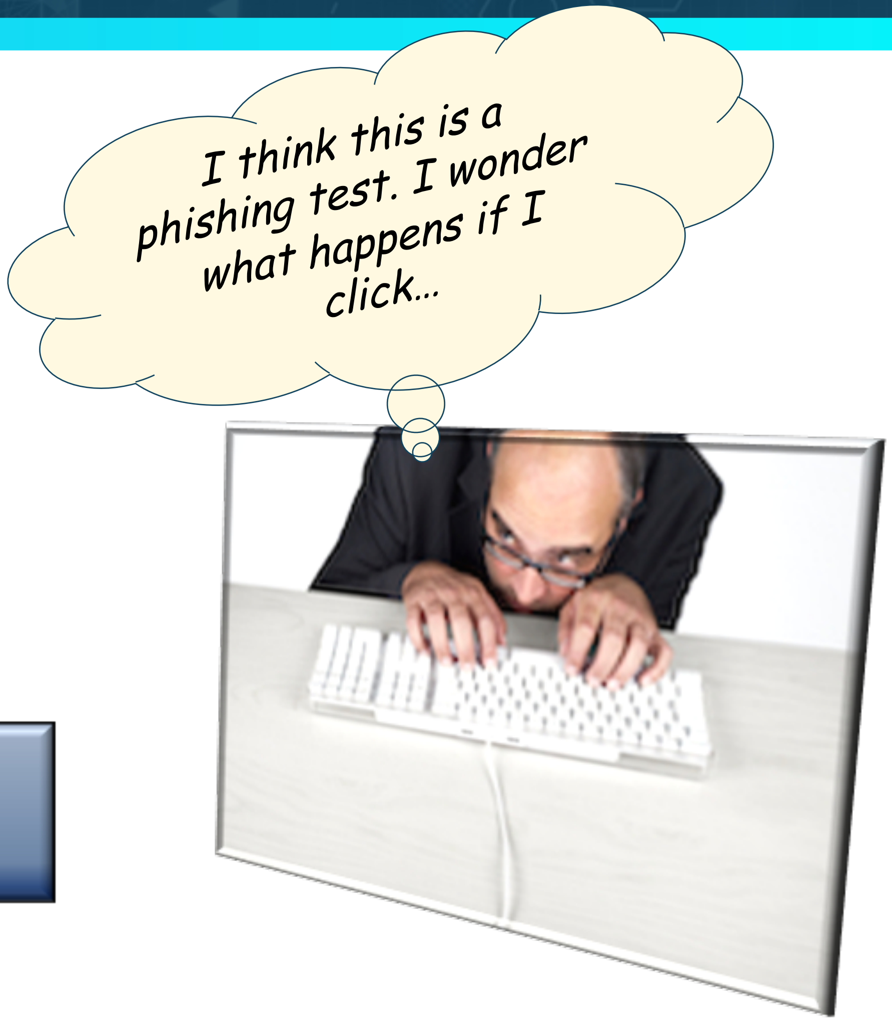
OK. These areas are "off-limits"…

…***payroll, helpdesk, executives***…

Book a Call

Pitfall #9: Curious and rebellious employees

- Keeping summary results secret can lead to **more clicks**
  - ***And will "clickers" send out warnings?***
- **Communicate aggregate results** soon after live tests, before they get restless


I think this is a phishing test. I wonder what happens if I click…

Are people clicking intentionally?

Pitfall #10: Lack of handling guidelines

Clues to spotting suspicious email messages, and what to do with a suspicious message:

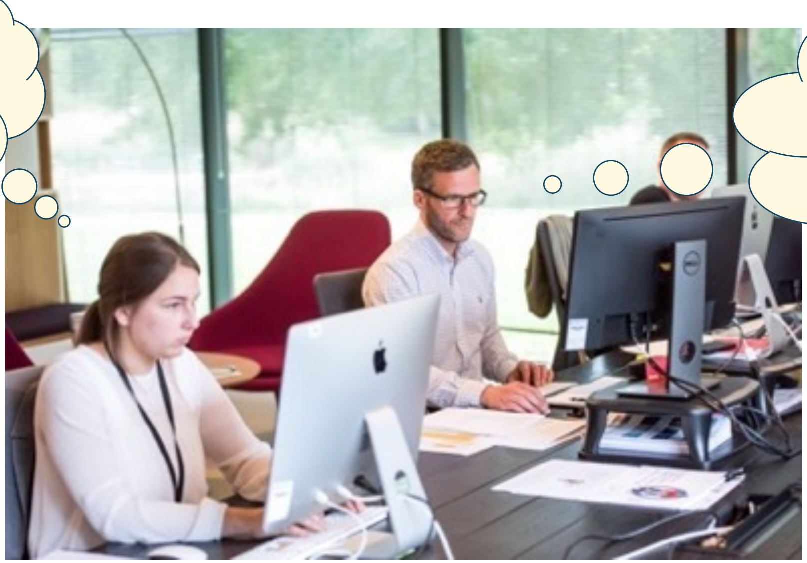
1. The message requests personal information by reply, or by entry into a form
2. The message requests that the recipient take urgent action.
3. The message contains simple grammar and spelling errors; or may contain wordings that are not commonly used
4. The message contains offers or describes situations that are too good to be true.
5. The message contains improper links that don't match the organization being represented.
6. The message is sent from a free webmail account that doesn't match the organization being represented.
7. Use the "phish hook" tool in your email client to report suspected phishing messages.
8. No need to report spam that is clearly not legitimate. Just delete it.

Have you taught people the basics, so there are fair expectations of what they should do?

Book a Call

Pitfall #11: Easily spotted tests (no need for people to analyze)

- If one test is good, more of them is better… right? (*Not necessarily*)
  - *More "variable" data is NOT good.*
- More frequent tests can become **adversarial**… ***and predictable***.



Are people getting to used to your testing patterns and easy clues that it's a test?

Phishing Assessment Pitfalls
1. Unpredictable employee actions
2. Impossibly difficult test messages
3. Embarrassing your employees
4. Employee confidentiality risks
5. Employee targeting backlash
6. Uncooperative spam filters
7. Spurious message difficulty
8. Forbidden Hot Button Impersonations
9. Curious and rebellious employees
10. Lack of handling guidelines
11. Easily spotted tests

And (#12) what do those who “don’t click” actually learn?

Teachable Moments?

Vulnerability Metrics?

Business Productivity?

Cultural Repurcussions?

Is “live phishing simulation” really the answer?

WWW.CLICKARMOR.CA

Book a Call

http://twitter.com/clickarmor

Reflecting on how to get better results…

When you consider how your effort spent in trying to avoid many of these undesirable outcomes is really making it hard to get the results you want, you can't help but wonder…

Isn't there a better way to measure vulnerability and teach employees not to click on dangerous links?

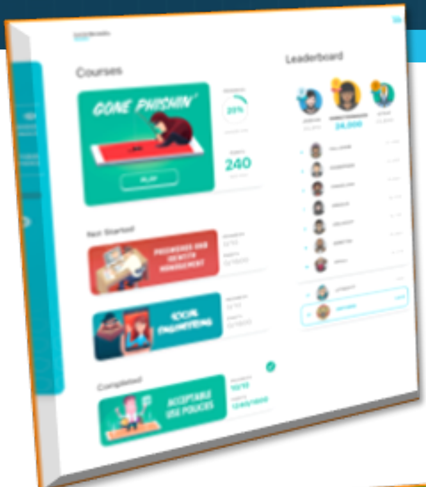
This is exactly what I was thinking a few years ago, and that's why I designed Click Armor to be a more positive, more consistent environment for doing all of this, all within in an easier process.

In fact, Click Armor provides a fully gamified platform that can be used to test and improve employees' resistance to **ANY** kind of threat. Why not book a call, get a demo, and benefit from the insights I've learned the hard way.

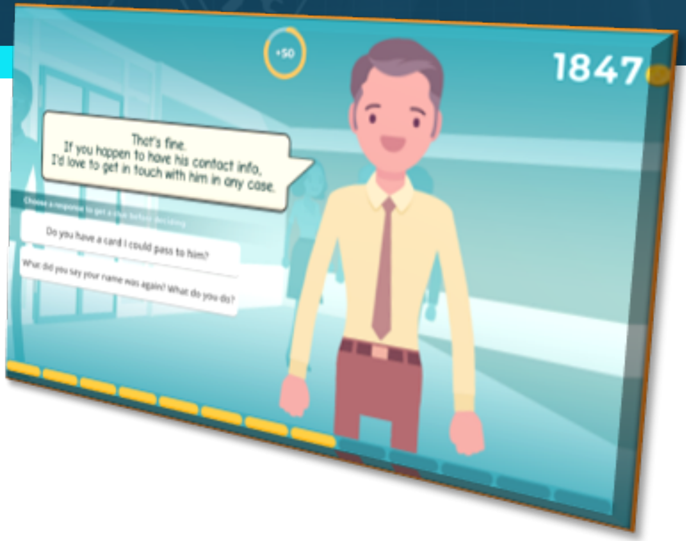
Scott Wright, CISA
CEO and Founder
Click Armor

Book a Call

What about the benefits of "Gamified Learning and Assessment?"



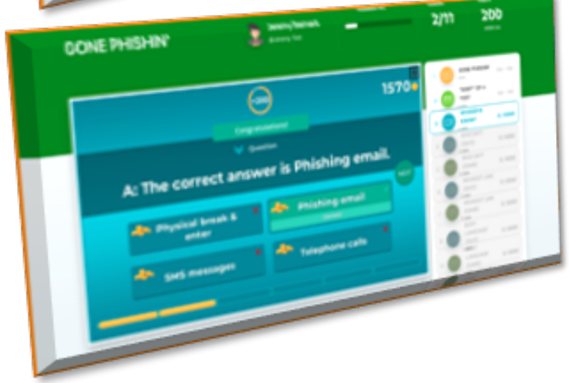
1. *Engagement is a positive experience*
2. *Interactive challenges reinforce knowledge*
3. *Scoring and leaderboards drive practice*
4. *Gamified simulations develop skills*
5. *Relevant assessments provide rich data*



That's fine.
If you happen to have his contact info.
I'd love to get in touch with him in any case.

Do you have a card I could pass to him?

What did you say your name was again? What do you do?



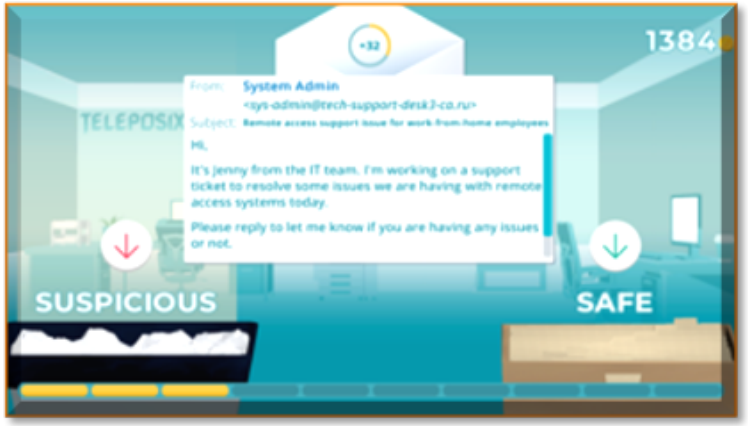
A: The correct answer is Phishing email.

Physical break & enter

Phishing email

SMS messages

Telephone calls



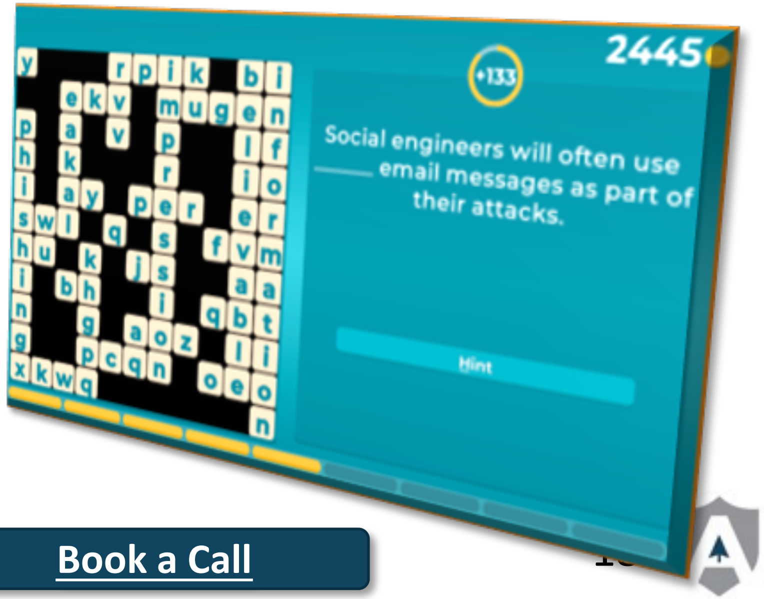
From: System Admin <sys-admin@tech-support-desk3-co.ru>

Subject: Remote access support issue for work-from-home employees

Hi,

It's Jenny from the IT team. I'm working on a support ticket to resolve some issues we are having with remote access systems today.

Please reply to let me know if you are having any issues or not.



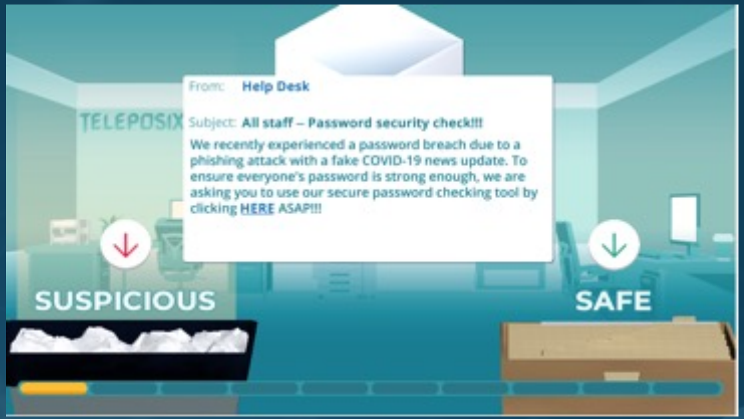
Social engineers will often use ______ email messages as part of their attacks.

Book a Call

ASSESS YOUR PHISHING VULNERABILITY TODAY WITH...
"CAN I BE PHISHED?"

Start Personal Gamified Phishing Assessment Now

Request a Free Team Phishing Assessment

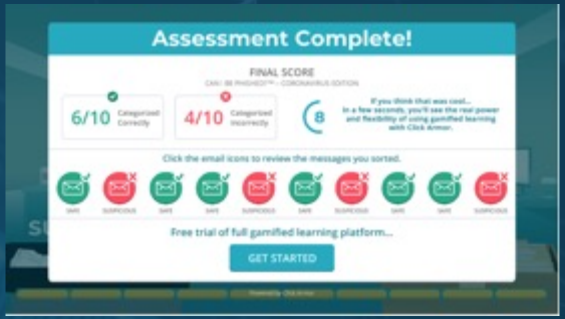


From: Help Desk

Subject: All staff – Password security check!!!

We recently experienced a password breach due to a phishing attack with a fake COVID-19 news update. To ensure everyone's password is strong enough, we are asking you to use our secure password checking tool by clicking HERE ASAP!!!

The agency said you could help me get caught up on things, as the COVID-19 pandemic has really set us back.
The first thing I need you to do is clear my backlog of email.
BACK
But I think you'll need to be pretty careful, as we've had a big increase in phishing messages from attackers trying to break into our network, and social engineers trying to scam our people.
NEXT



Assessment Complete!

FINAL SCORE

CAN I BE PHISHED™ – CORONAVIRUS EDITION

6/10 Categorized Correctly

4/10 Categorized Incorrectly

8 If you think that was cool... In a few seconds, you'll see the real power and flexibility of using gamified learning with Click Armor.

Click the email icons to review the messages you sorted.

Free trial of full gamified learning platform...

GET STARTED

Try our 3-minute self-assessment at:
http://canibephished.com

WWW.CLICKARMOR.CA

Book a Call

http://twitter.com/clickarmor

Level up from "live phishing tests" to "Gamified Learning & Simulations"

1. **More engaging**
2. **Less firewall/gateway hassle**
3. **More testing scope**
4. **More culture-friendly**
5. **More consistent**
6. **More versatile**

7. Much more useful data!

That's fine.
If you happen to have his contact info,
I'd love to get in touch with him in any case.

Do you have a card I could pass to him?

What did you say your name was again? What do you do?

A: The correct answer is Phishing email.

Social engineers will often use email messages as part of their attacks.

From: System Admin <sys-admin@tech-support-desk3-cs.ru>

Subject: Remote access support issue for work from home employees

Hi,

It's Jenny from the IT team. I'm working on a support ticket to resolve some issues we are having with remote access systems today.

Please reply to let me know if you are having any issues or not.

Want to know more about
Gamified Phishing Assessments?

Book a Demo