Microsoft

Using DMARC to improve your email reputation

Terry Zink
Program Manager

Outline

1. The problem
2. How does DMARC work?
3. The unexpected upside of DMARC
4. The unexpected downside of DMARC
5. Case study
6. Conclusion

Outline

1. The problem
2. How does DMARC work?
3. The unexpected upside of DMARC
4. The unexpected downside of DMARC
5. Case study
6. Conclusion

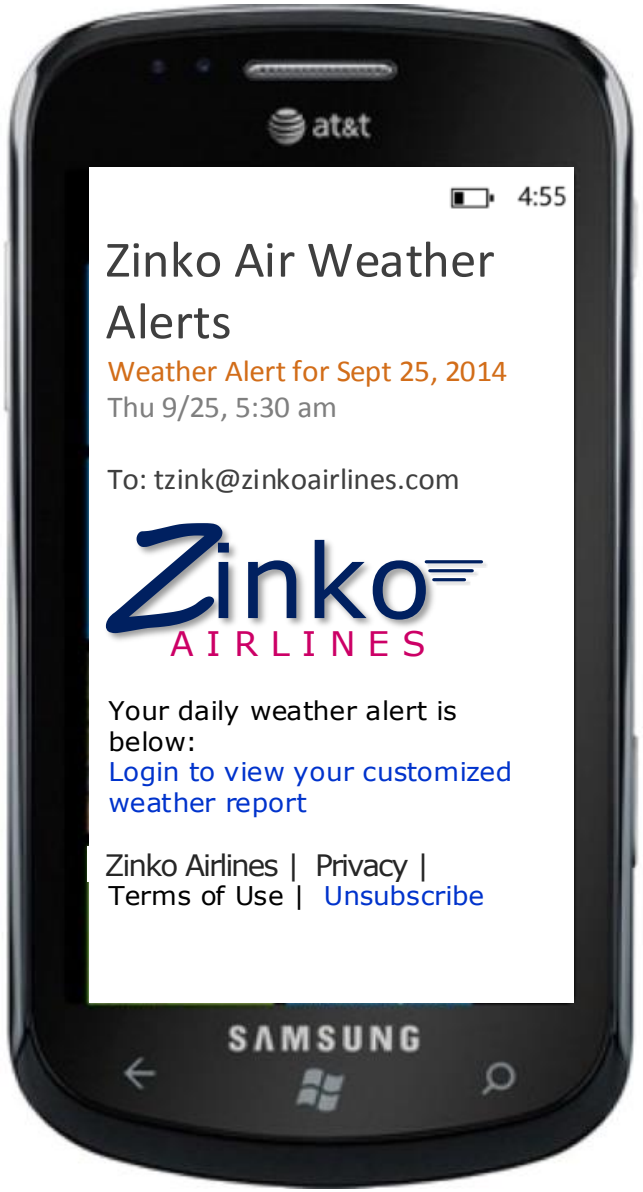
Meet "Tom"

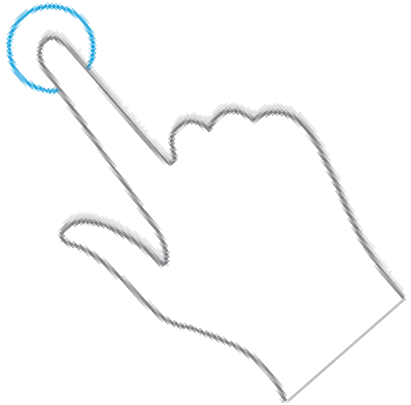
Tom's a pilot for Zinko Airlines. He flies mostly commercial passenger jets but occasionally he does private jets in his spare time.

He's a very responsible pilot. He reads his manifests, checks the weather and forecasts ahead of time, and ensures that people have a smooth flight. He gets weather alerts every morning.

Zinko AIRLINES

Why is phishing so hard to detect?



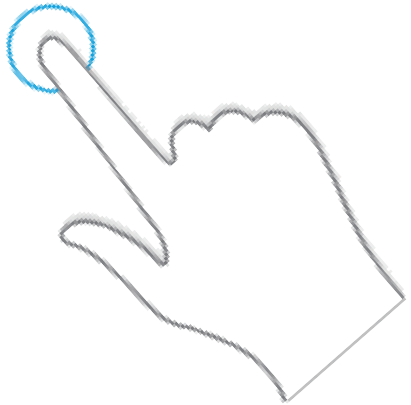


One day, Tom gets an email from Zinko Airlines's daily weather alert service.

He clicks the link to go to the company's internal website where they have the daily schedule and weather information.

Why is phishing so hard to detect?

Close, but not the right URL!



He enters in his information to login and receives a login failure. He is directed back to the company's web page where he logs in again.

But the damage has been done. Tom has been fooled into surrendering his login credentials to a phisher.

Why is phishing so hard to detect?

1. Looks like the real thing
2. Hard for users to notice anything that is “off”
3. Traditional anti-spam techniques don’t work

Why is phishing so hard to detect?

1. Looks like the real thing
2. Hard for users to notice anything that is "off"
3. Traditional anti-spam techniques don't work

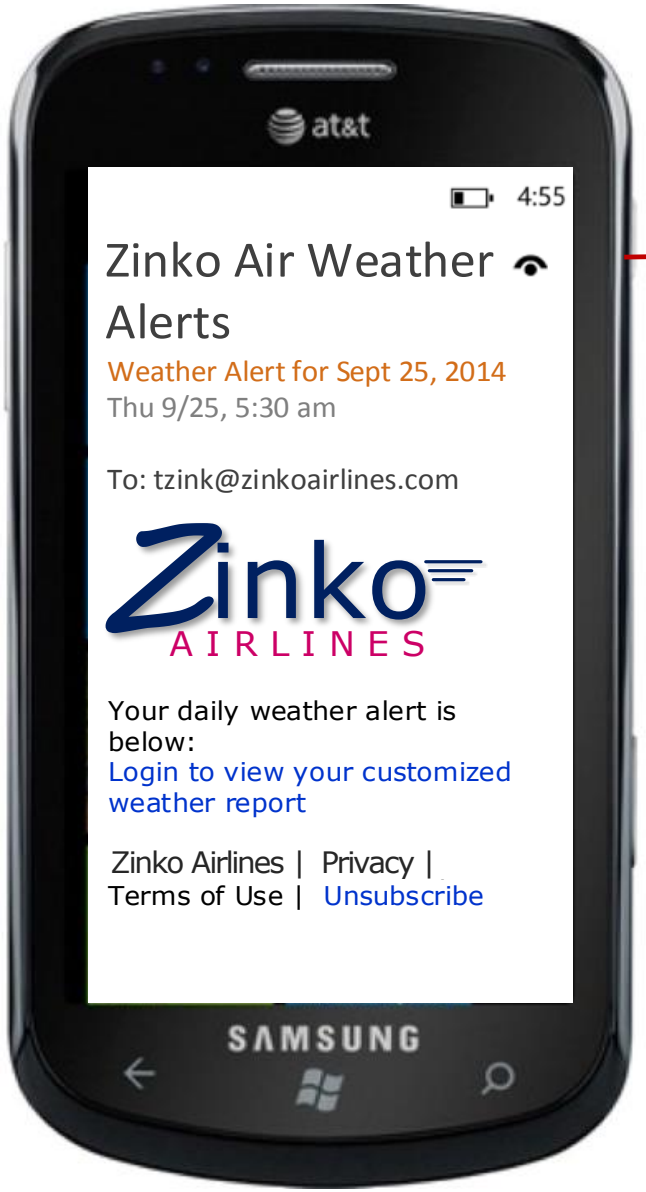
Anti-abuse techniques usually focus on the filter to sort out good email from spam; however, phishing has the following characteristics:

a) Sent from IP addresses and/or domains that don't have previous bad reputation
b) Domains may authenticate with SPF or DKIM but this is hidden from the user
c) Even the 5322.From may be hidden from the user, depending on the email client

Outline

1. The problem
2. How does DMARC work?
3. The unexpected upside of DMARC
4. The unexpected downside of DMARC
5. Case study
6. Conclusion

How DMARC stops phishing



From: Zinko Air Weather Alerts <alerts@alerts.zinkoair.com>

↓

Does alerts.zinkoair.com have a DMARC policy? Yes.

↓

Does this message authenticate? Yes.

↓

Does authenticated domain align with what user sees?

↓

If No, this message fails DMARC and the receiver can choose to do nothing, mark as spam, or reject it

Outline

1. The problem
2. How does DMARC work?
3. The unexpected upside of DMARC
4. The unexpected downside of DMARC
5. Case study
6. Conclusion

Balancing security vs functionality

Fixing the phishing problem

Not losing important email

Feedback

1. Collect feedback
2. Detect misconfigurations
3. Inventory 3rd party mailers
4. Authenticate all your email!

Detect Malicious Spoofing

1. Spammer on the Internet sends an email spoofing joe@example.com

2. Message does not pass DKIM or SPF, fails DMARC, mark message as spam

Mail filter

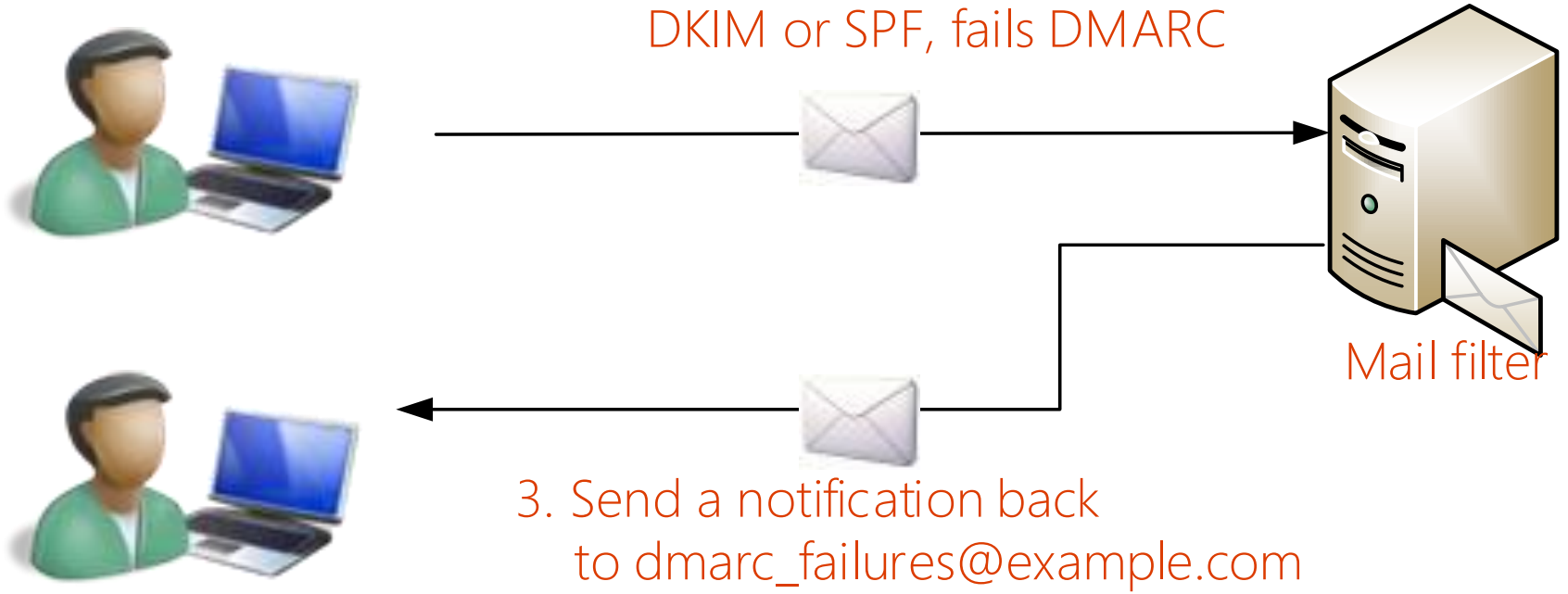
3. Send a notification back to dmarc_failures@example.com

4. Admins at example.com investigate the spammer “Hmm, someone is spoofing me!”

Detect Misconfigurations

1. joe@example.com sends a message from a new set of servers

2. Message does not pass DKIM or SPF, fails DMARC



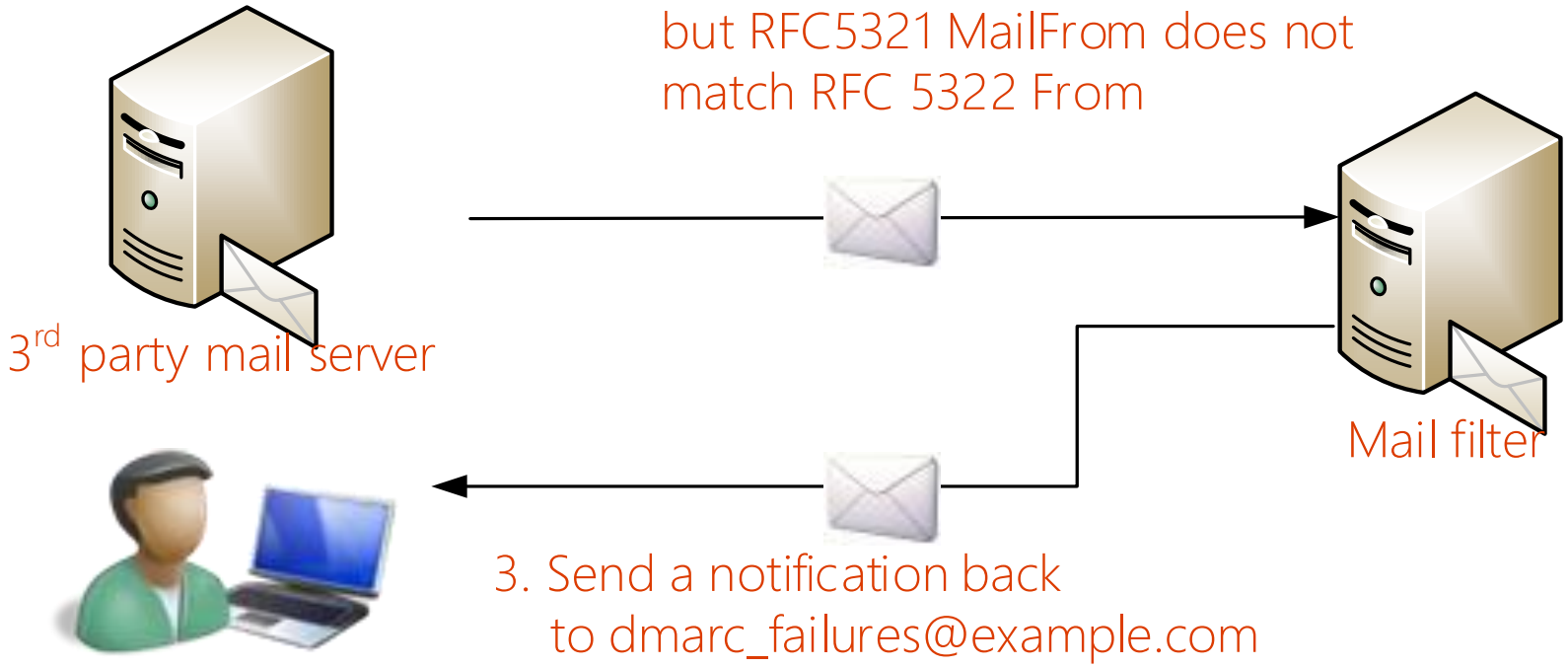
3. Send a notification back to dmarc_failures@example.com

4. “Oops, I forgot to add this machine’s IPs to my SPF record, and forgot to enable DKIM.”

Inventory 3rd Party Emailers

1. 3rd party mail server sends MAIL FROM alerts@3rdParty.com, From: alerts@example.com

2. Message passes SPF and DKIM, but RFC5321 MailFrom does not match RFC 5322 From

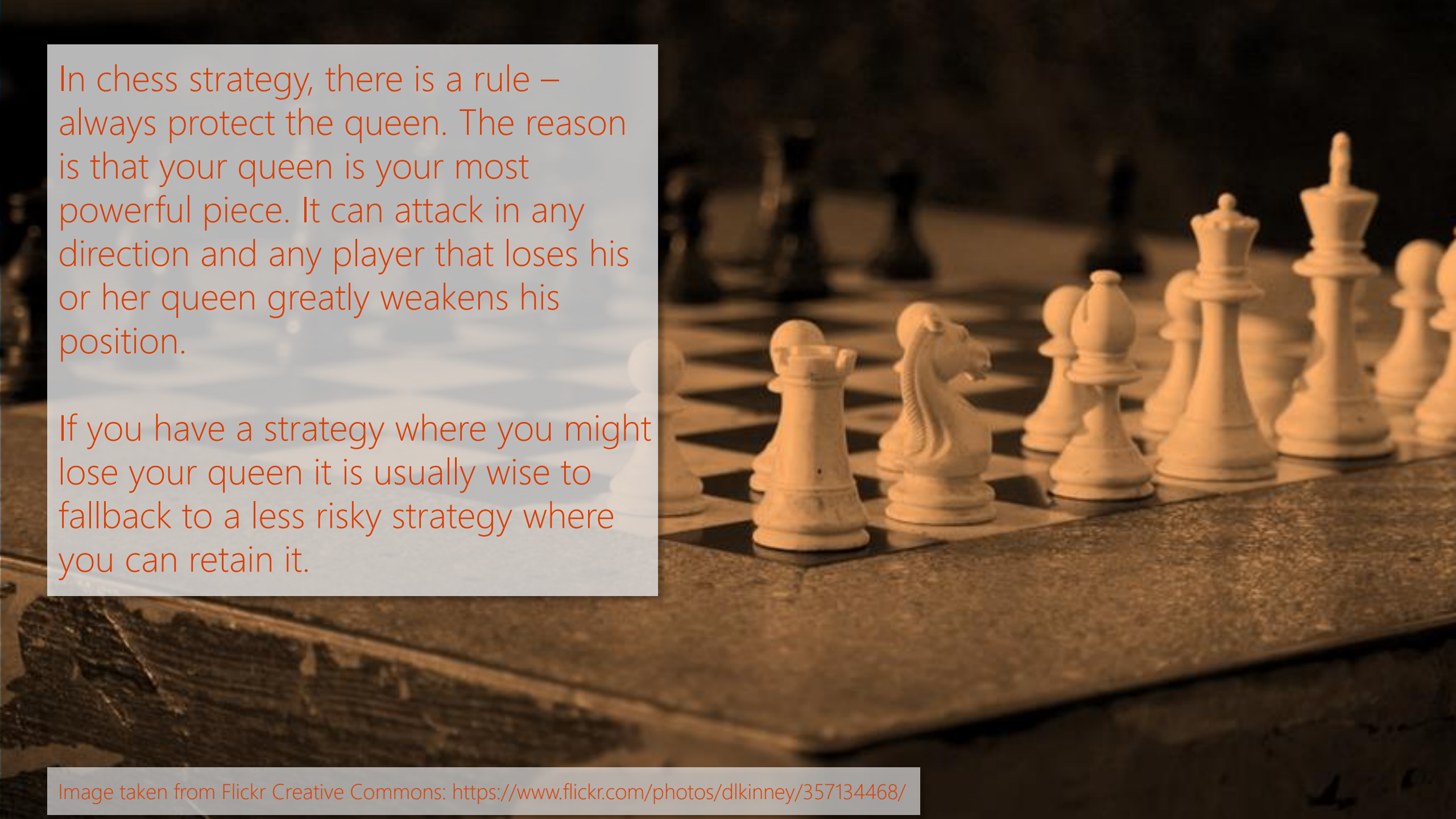


3. Send a notification back to dmarc_failures@example.com

4. "Oops, I forgot to delegate a subdomain to this 3rd party mailer like Terry Zink explained on his blog."

Outline

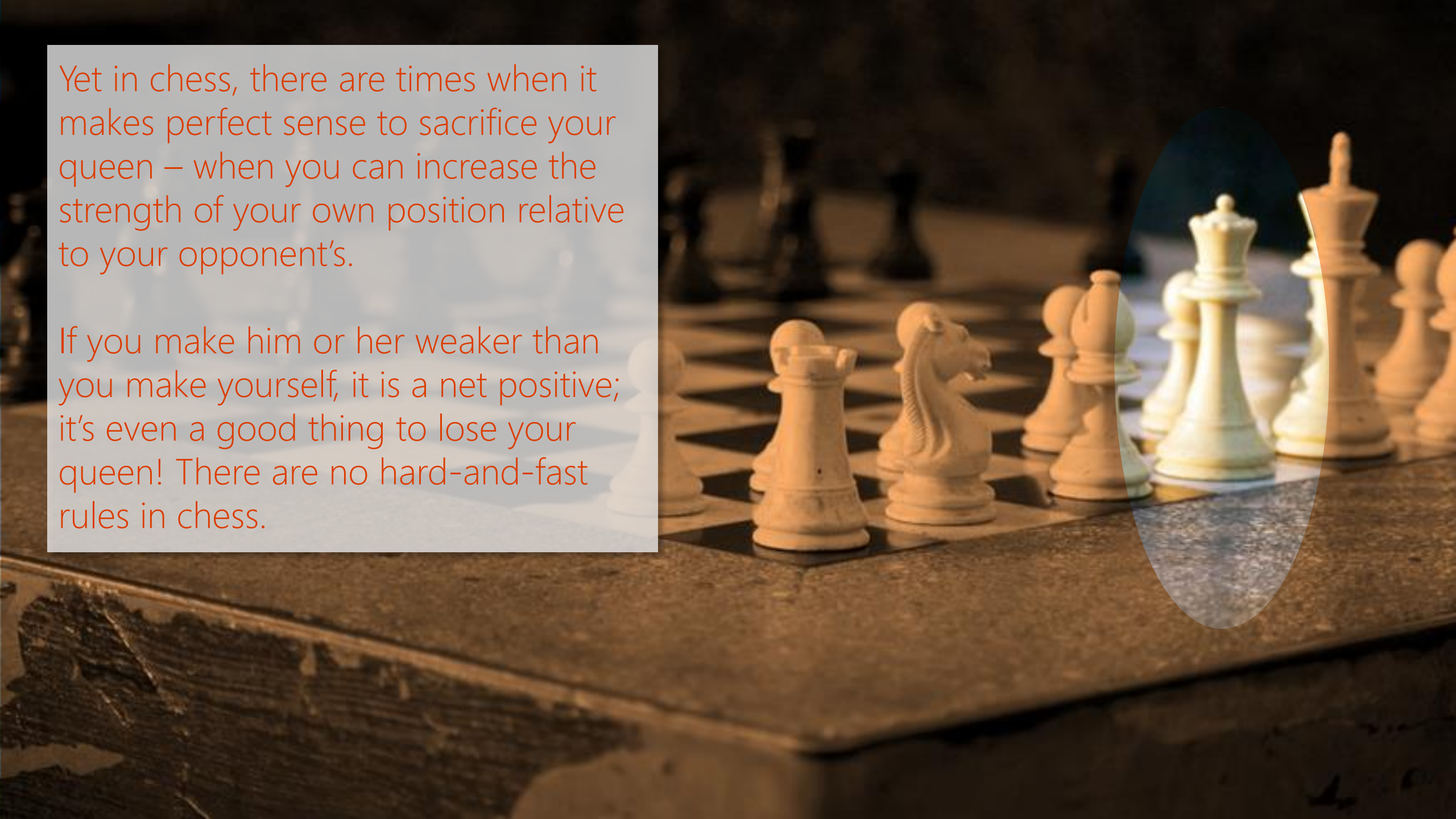
1. The problem
2. How does DMARC work?
3. The unexpected upside of DMARC
4. The unexpected downside of DMARC
5. Case study
6. Conclusion



In chess strategy, there is a rule – always protect the queen. The reason is that your queen is your most powerful piece. It can attack in any direction and any player that loses his or her queen greatly weakens his position.

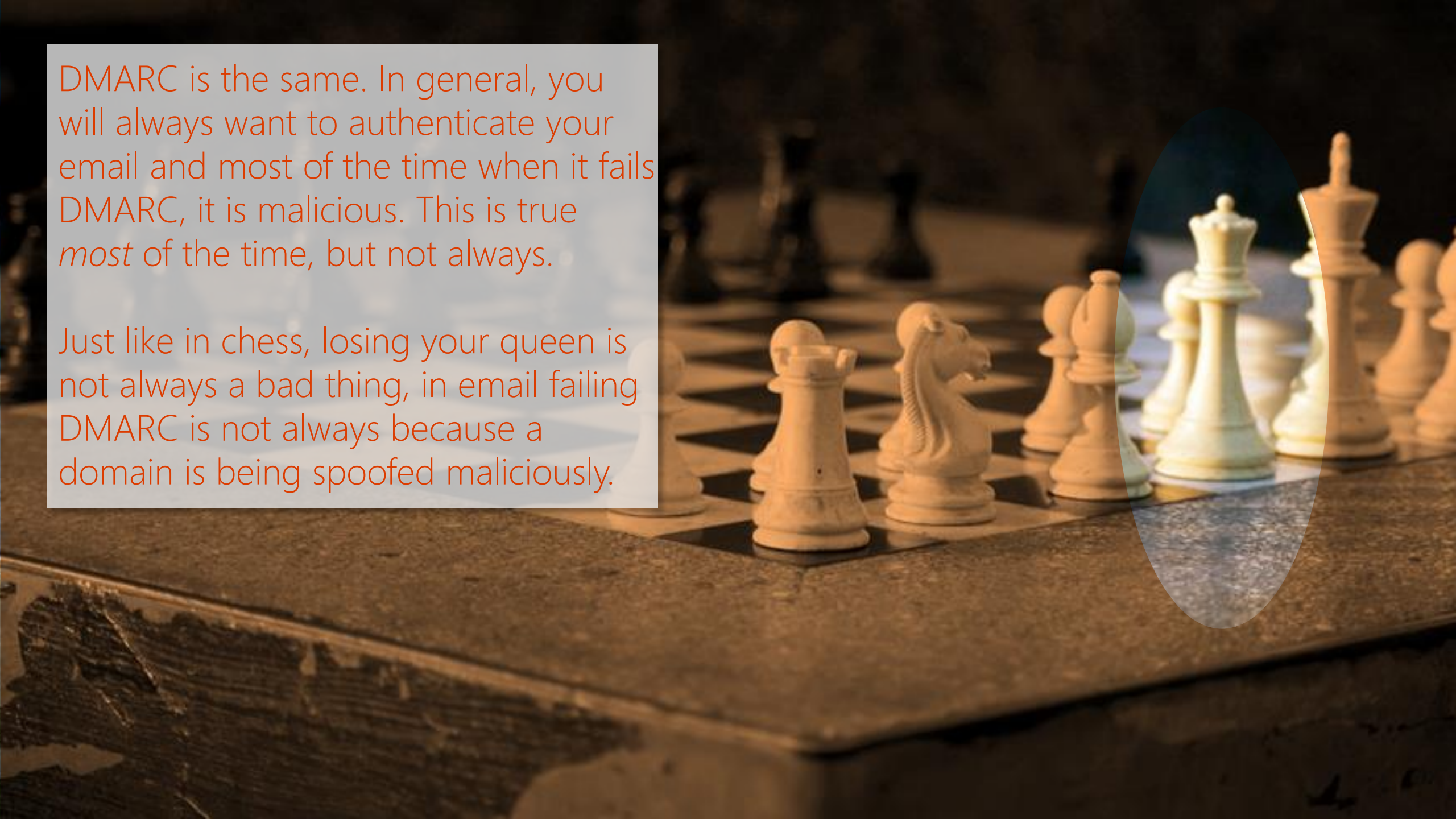
If you have a strategy where you might lose your queen it is usually wise to fallback to a less risky strategy where you can retain it.

Image taken from Flickr Creative Commons: https://www.flickr.com/photos/dlkinney/357134468/



Yet in chess, there are times when it makes perfect sense to sacrifice your queen – when you can increase the strength of your own position relative to your opponent's.

If you make him or her weaker than you make yourself, it is a net positive; it's even a good thing to lose your queen! There are no hard-and-fast rules in chess.



DMARC is the same. In general, you will always want to authenticate your email and most of the time when it fails DMARC, it is malicious. This is true *most* of the time, but not always.

Just like in chess, losing your queen is not always a bad thing, in email failing DMARC is not always because a domain is being spoofed maliciously.

Breaking the chain

Case 1: SPF only works if the message originates here

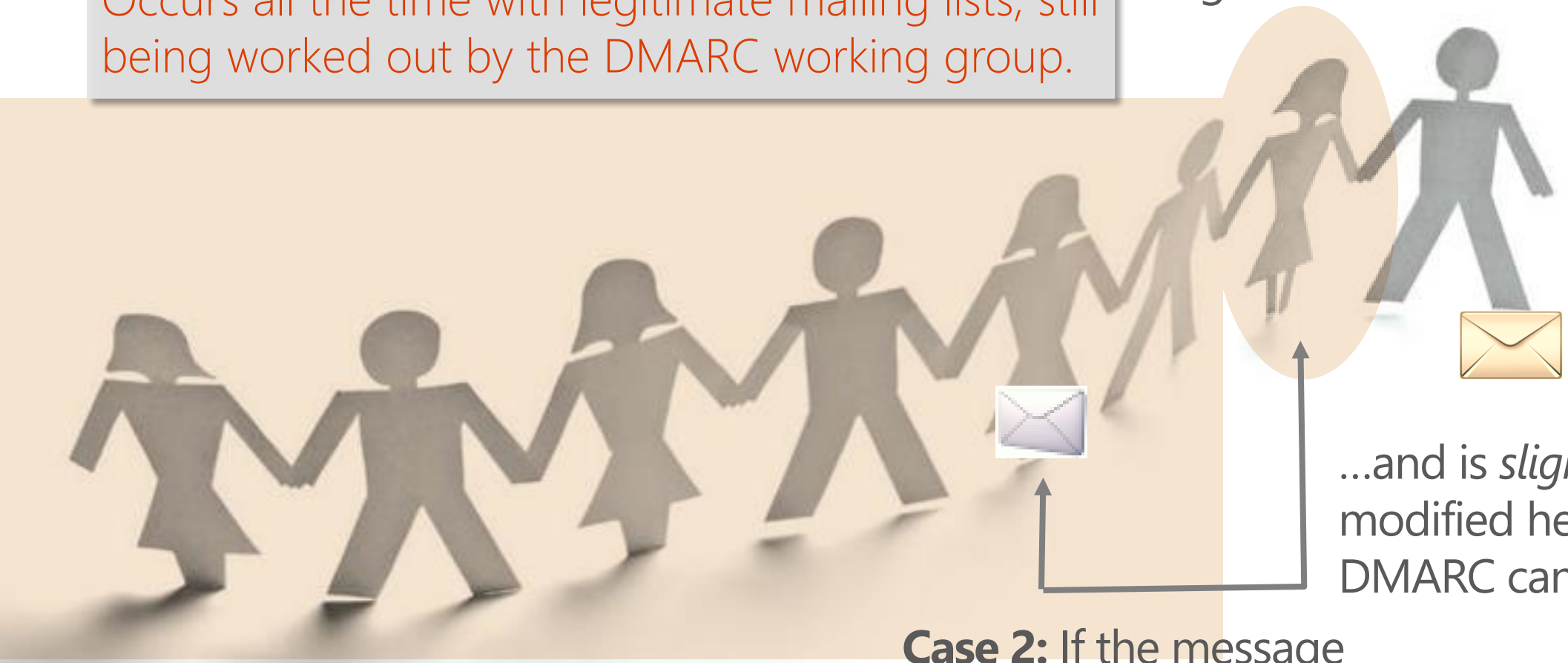
…and is *slightly* modified here, DMARC can break

Case 2: If the message originates here…

Breaking the chain

Occurs all the time with legitimate mailing lists, still being worked out by the DMARC working group.

Case 1: SPF only works if the message originates here



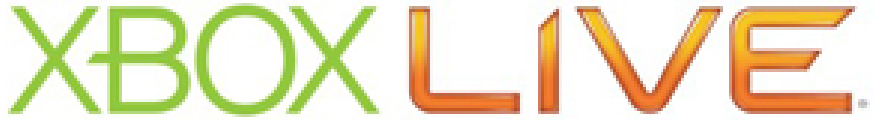
…and is *slightly* modified here, DMARC can break

Case 2: If the message originates here…

Outline

1. The problem
2. How does DMARC work?
3. The unexpected upside of DMARC
4. The unexpected downside of DMARC
5. Case study
6. Conclusion

Case study: Microsoft Corporation



Case study: Microsoft Corporation

Step 1 – Microsoft decided how to receive DMARC reports (used a 3rd party)

Step 2 – Published a DMARC record

Step 3 – Sorted through the DMARC reports for IPs that are used for corporate traffic

Step 4 – Sorted through the DMARC reports for IPs that are internal to the company but failing authentication

Step 5 – Sorted through the DMARC reports for IPs that are external to the company and failing authentication.

Case study: Microsoft Corporation

Step 6 – Got all the internal teams to properly authenticate email (about 30 of them)

Step 7 – Updated DKIM keys

Step 8 – Update the SPF record to a hard fail, now more difficult for spammers to spoof Microsoft

Step 9 – Next: Publish a DMARC record of p=quarantine

Conclusion

1. DMARC solves one aspect of phishing
2. DMARC lets domains be more secure
3. But, DMARC still has challenges that are not yet solved

© 2014 Microsoft Corporation. All rights reserved. Microsoft, Windows, Windows Vista and other product names are or may be registered trademarks and/or trademarks in the U.S. and/or other countries.
The information herein is for informational purposes only and represents the current view of Microsoft Corporation as of the date of this presentation. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information provided after the date of this presentation. MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS PRESENTATION.