riskalyze

Is Your Client Data Safe?

3 Cybersecurity Tips for Advisors

Anyone that keeps up with news knows that cyber attacks and other security threats are on the rise. Big companies (with big cybersecurity budgets to match) weren't even safe from the Wanna-Cry and GoldenEye ransomware attacks in May/June. And we're just getting started with Equifax. With over 143 million Americans compromised in that hack, advisors will need to continue being vigilant in the wake of that fiasco for years to come.

Hackers are getting more sophisticated and it's not enough to sit behind a firewall or an IT budget anymore. Protecting sensitive information is a top priority, now more than ever. What can you do to protect your clients and their assets?

As technology evolves, so do the risks. We put together three easy ways to stay ahead of the curve. We've also included links to security resources at the end for you to stay informed on the latest developments from FINRA and the SEC.

Learn to Identify Threats

Most cyber attacks originate from humble sources: a link, an email, or an attachment. As hackers keep finding ways to circumvent spam filters, it gets harder to identify which items are safe and which are going to make you "WannaCry." An internal "Best Practices" guide is an effective first step for your security strategy, and it doesn't have to be complicated. Keeping a simple list of common scams can be an effective way to increase awareness in your firm.

Make sure every member of your team knows these three common threats:

Phishing: emails that *appear* to come from reputable companies in order to steal personal information, such as passwords and credit card numbers.

Example:


Hi there,

Wilson has shared a document "**Signed Wire Payment Receipt.pdf**" on Dropbox with you.

View Document Now

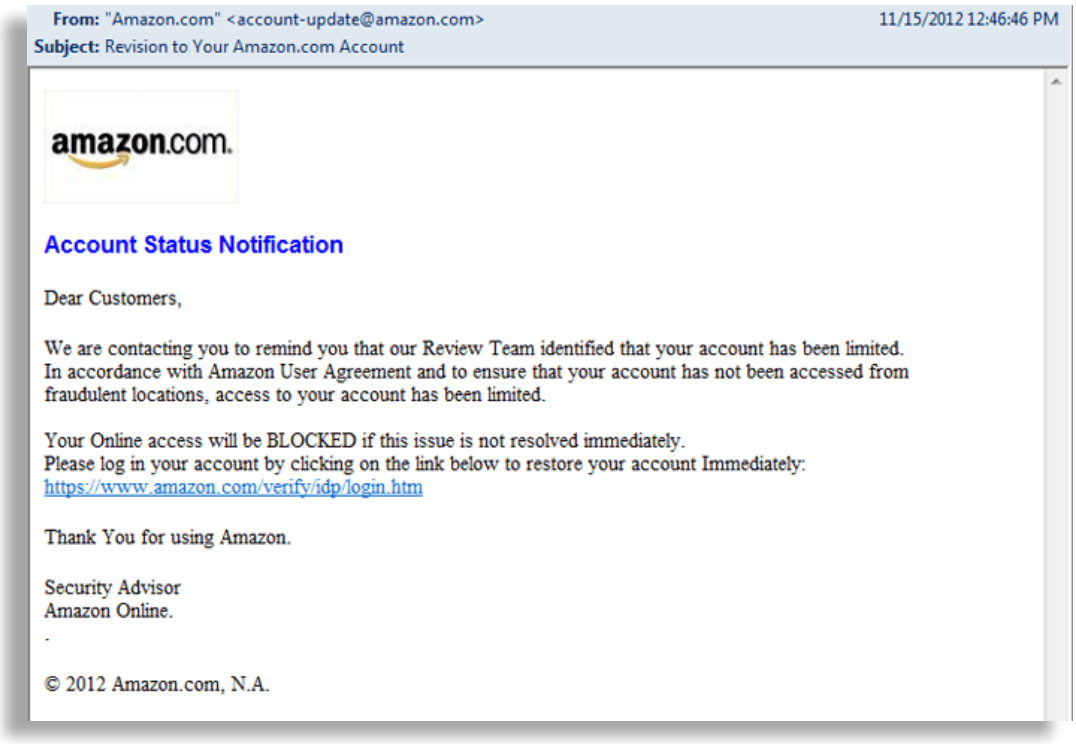
Documents will be removed from our system upon the request of the sender.

Enjoy!
The Dropbox team

The example above appears to be from Dropbox, a well-known company your firm might use regularly. But notice the inconsistencies: the wrong fonts, lack of branding, and a format that doesn't have the polish of the Dropbox emails you usually get. Watch out for sender domains that are close—"@dorpbox.com" might not look alarming at first glance! Have other members of your team look out for these subtle details and, **when in doubt, don't click.**

Spoofing: another form of phishing email where the "sender" address has been forged, making them *appear* to come from legitimate companies.

Example:



From: "Amazon.com" <account-update@amazon.com> 11/15/2012 12:46:46 PM
Subject: Revision to Your Amazon.com Account

amazon.com.

Account Status Notification

Dear Customers,

We are contacting you to remind you that our Review Team identified that your account has been limited.
In accordance with Amazon User Agreement and to ensure that your account has not been accessed from fraudulent locations, access to your account has been limited.

Your Online access will be BLOCKED if this issue is not resolved immediately.
Please log in your account by clicking on the link below to restore your account Immediately:
https://www.amazon.com/verify/idp/login.htm

Thank You for using Amazon.

Security Advisor
Amazon Online.
-

© 2012 Amazon.com, N.A.

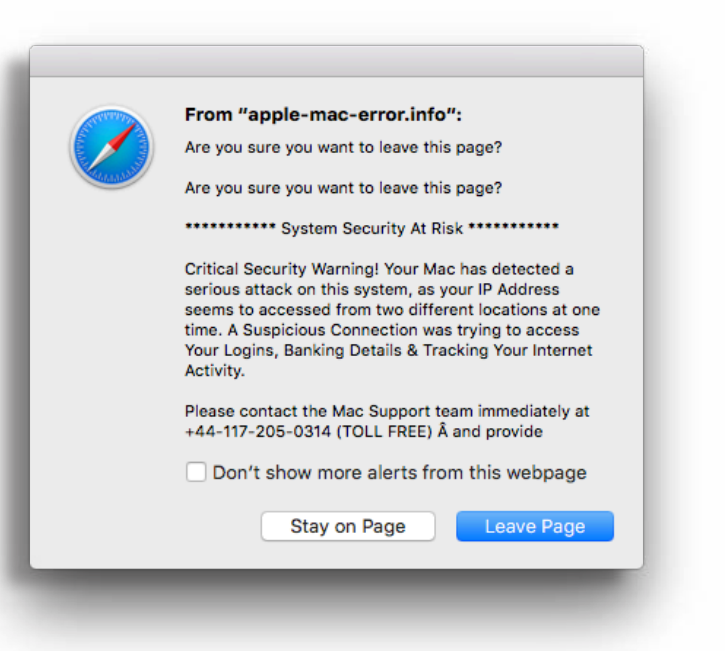
Spoofing is a type of phishing scam in which the email header has been modified so that it appears to come from a well-established domain. In the example above, the email address has the domain "amazon.com." Tell-tale signs like bizarre branding, typos, or suspicious language could tip you off, but what if these signs aren't so obvious? How do you know if a message is legit? The truth is, you may not always know.

Here's the rule of thumb: unless you've requested a specific email (a password reset, for example), you don't need to access accounts through the emails that alert you to them. If you've got the tiniest shred of doubt, open a new browser tab or window and log in directly. If you have an account that needs attention, address it inside a secure site! (Pro tip: most modern browsers place a lock symbol next to URLs to signal a "secure certificate.")

Hackers are able to spoof email addresses when websites don't have domain protection. If your website doesn't have direct domain security, spammers can hijack your site address and send spoofing emails in your name. Go over your security settings with your site host so you don't end up an accidental spammer yourself.

Pop-ups: a window that appears on a website prompting for sensitive information or indicating a security issue.

Example:



Pop-ups are the elder statesmen of spam, but they can still wreak havoc if you're not careful. As before, keep a look out for strange branding or an increased sense of urgency that seems out of character. Luckily, the majority of these eyesores are wiped out with a good quality pop-up blocker. Continue to keep an eye out for intrusive messages and install a pop-up blocker if there isn't one already included in your antivirus software.

Once a suspicious link or email is clicked, you're looking at a laundry-list of headaches with no easy (or cheap) fix. One thing to keep in mind is that security is only as strong as it's weakest link. Hackers need to enter through just one computer in order to take over an entire network. Make sure that everyone with internet access has examples of these common threats. Security incidents usually happen because well-intentioned advisors weren't vigilant.

Say "Yes" to the Cloud

One of the big lessons to be learned from the WannaCry and GoldenEye attacks is that data stored on a personal computer is vulnerable. Victims were forced to pay a bitcoin "ransom" in order to retrieve their files, and with GoldenEye, those that paid the ransom had their data wiped anyway. WannaCry hackers were able to collect nearly $32,000 before the threat was squashed.

If your data can only be accessed from your computer, you're opening yourself up to cyber blackmail.

Luckily, modern CRMs and other fintech providers store information securely for you in 3rd party or cloud-based servers. For advisors who secure client data this way, WannaCry wasn't a big threat. The lesson to be learned is that a local hard drive, no matter how many firewalls it sits behind, isn't entirely safe.

Ask Your Vendors About Security

As vigilant as you are at keeping your client's information safe, expect the same from your technology vendors. Fintech companies that manage your data undergo increased scrutiny and have rigid safeguards in place. Don't be afraid to ask about them!

At Riskalyze, we have a section of our website fully dedicated to security and privacy. We take security seriously and prove it. With any tech provider, ask them questions to understand how they handle your information:

- **Do your employees undergo background checks and security information training?**
- **Where are your data centers located and what certifications do they have?**
- **Do you share data with third parties?**

We hope these tips are a helpful addition to the measures your firm already takes to navigate this new era of cyber threats.

For additional reading, check out the FINRA Cybersecurity Checklist and the SEC IM Guidance Update.

To see how Riskalyze is keeping your data safe, check out the security section of our website.

ABOUT RISKALYZE

Riskalyze is the company that invented the Risk Number®, which powers the world's first Risk Alignment Platform, empowers advisors to automate client accounts with Autopilot, and enables compliance teams to spot issues, develop real-time visibility and navigate changing fiduciary rules with Compliance Cloud. Advisors, broker-dealers, RIAs, asset managers, custodians and clearing firms use Riskalyze to empower the world to invest fearlessly. To learn more, visit www.riskalyze.com.

Riskalyze
373 Elm Avenue
Auburn, CA 95603

855-RISKALYZE
530-748-1660
Fax 530-748-1661

Follow @Riskalyze