PHISHING
FIELD GUIDE

How to Keep Your Users Off the Hook

Barkly™

Table of Contents

Introduction

Gone Phishing

Jack Danahy, co-founder and CTO at Barkly

Twenty years ago, hackers attempted to breach organizations by breaking holes (or finding them) in the network perimeter of organizations, or in exposed and critical servers. In response, security became focused on locking those things down. The result: a "hard, crunchy outside" that unfortunately still left internal users, systems, and networks unprotected.

Modern attackers have long since realized the easiest way to deliver their attack tools is to focus on the "soft, chewy, center" of the organization. And the very softest part is the ambulatory, 98.6 degree system: the user.

Users are susceptible to all manner of phishing cons, from free software to fake websites, from unsolicited photos to Nigerian fortunes. They unwittingly type their credentials into fraudulent screens. They click on malicious links that install system monitors, ransomware, backdoors, and bots. It's hard to blame them. Social networks, particularly LinkedIn and Facebook, serve up all the information, contacts, and backstory necessary to make a forged message look real. When that message appears to come from a high-level executive, it's very easy for any employee at an organization to be duped.

When the user interacts with these messages — getting hooked by the phishing attack — the attackers have everything they need to launch a much more substantial penetration. For these reasons, phishing has become the delivery vehicle for all manner of corruption. The cost of these attacks is in the hundreds of millions of dollars and mounting, and their profitability continues to spawn new criminals and increasingly sophisticated new tools.

Preventing these losses starts and ends with supporting the users — protecting them from themselves, and, while they develop better habits, protecting the organization from their mistakes. This guide will help you to develop and deliver messages that will raise the priority of security in the organizational mind. It will also give you some concrete steps to take in blunting the sharp edge of the phishing trend and its dangers. Weakness has taught attackers to phish. Now it's time to teach our users to resist the lure.

HABITAT

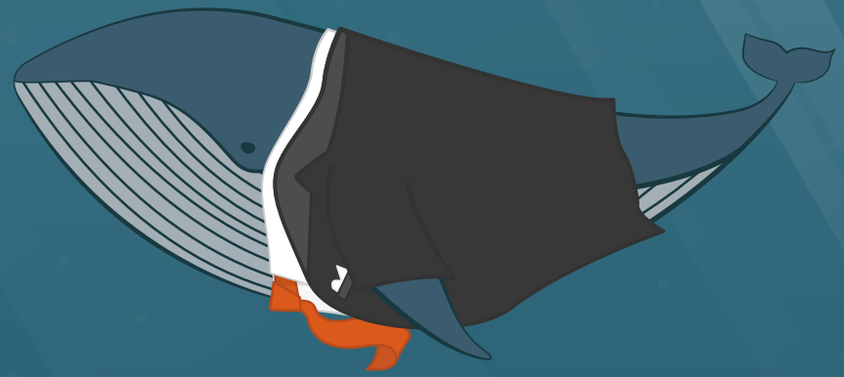
Corner Offices, Board Meetings, Conference Keynotes

PRIZED FOR

Confidential Information, Financial Data, Executive Credentials

FREQUENCY

Rare



The Executive

"The Whale"

Big Shoticus Executatum

CEOs, CFOs, and other executives are some of the biggest phishing targets at your company. As high-ranking decision-makers, they're prized for their access to sensitive corporate information as well as their authority to sign-off on things like wire transfers.

Habitually busy and no strangers to urgent requests, executives often don't have time to closely inspect every email they get when they're rushing from one meeting to the next. Many have assistants to help them manage their day-to-day, and those employees can be popular phishing targets, too (more on them later).

Why & How Phishers Target Them:

Their authorization and access privileges make executives extremely popular — and potentially very lucrative — phishing targets. Because they have higher public profiles than lower-level employees, it's also often easier for attackers to find information online (executive team bios, LinkedIn connections, etc.) they can use to make their phishing emails more convincing and specific.

Phishing attacks on executives typically take the form of a request for sensitive information from a trusted source. It could be someone they regularly do business with, a fellow executive at their company, or even the CEO. By commandeering or spoofing a CEO's email, attackers can make requests to other executives that are far less likely to be turned down. After all, who says "no" to the boss?

How to Protect Them:

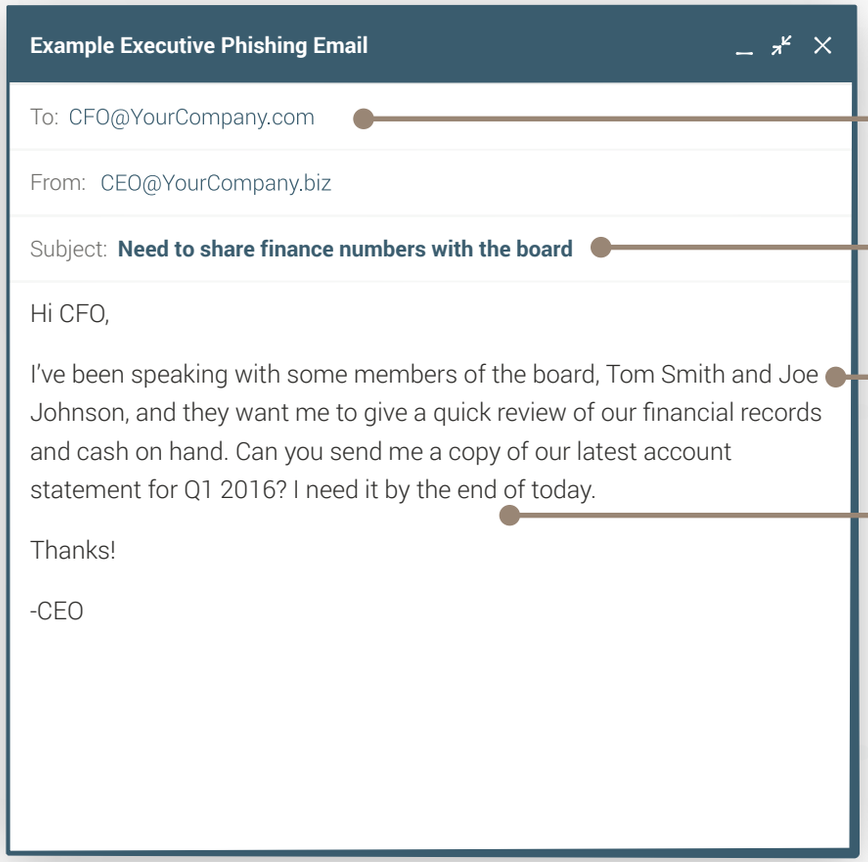
- Make additional authentication or verification steps required for any sensitive requests like wire transfers.
- Encourage execs to limit what they share and who they connect with on social networks.
- Make it policy not to share confidential information over email.

How to Be a "Whale Whisperer":

- Nothing gets executives' attention like reminding them how important they are. Explain why they're such prized targets. Underscore the havoc it can wreak on the company if they personally get compromised.
- Remember, with execs, numbers talk. Make the business case for mandatory security awareness training tailored specifically for them. Have stats ready to back yourself up.
- Try appealing to their leadership instinct by conducting company-wide phishing tests and making them accountable for improving their departments' results. For an added boost, make it competitive.

What A Phishing Email Might Look Like:

Here's an example of a phishing email your CFO might receive requesting he/she share financial information in advance of a board meeting.



Be on the lookout for domains that don't quite match up.

Follow up on any request for sensitive or confidential information by double-checking with the sender either by phone or in person.

Be skeptical of details like the names of board members — that information can easily be found on your company website

Don't fall for suspicious urgency. Deadlines like this are often used to discourage a target from verifying the sender.

HABITAT

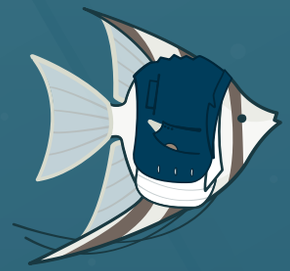
Front Desks, Company Functions, Anywhere a Whale is

PRIZED FOR

Access to Whales, Confidential Information, High Email Volume

FREQUENCY

Medium



Administrative Assistant

"Administrative Angelfish"

Knowicus Everythingilus

Masters of multitasking. Lords and ladies of logistics. Keepers of the calendar and phenoms of the phone screen. Administrative assistants are the unsung heroes of the corporate fish school. They handle all the behind-the-scenes scheduling, organizing, and gatekeeping that keeps everything running smoothly and enables executives to do their jobs.

Because of their supporting role, admin assistants often have access to company and individual executive accounts, and it's not uncommon for them to sign off on transactions or make payments on an executive's behalf. They take the job of managing their executives' time and day-to-day tasks very seriously, but they can also be habitually accommodating and deferential, not to mention in a rush.

Why & How Phishers Target Them:

With the possible exception of executives, admin assistants are some of the most highly-prized phishing targets in your organization. That's because, thanks to their close association with executives and access to their accounts, attackers tend to view them as softer targets who can still give up the keys to the kingdom.

Phishing attacks on administrative assistants often take the form of a request from another executive or a vendor they do business with. A common phishing tactic is to say the executive they support already approved a request and the admin just has to review an attachment or send along some information.

How to Protect Them:

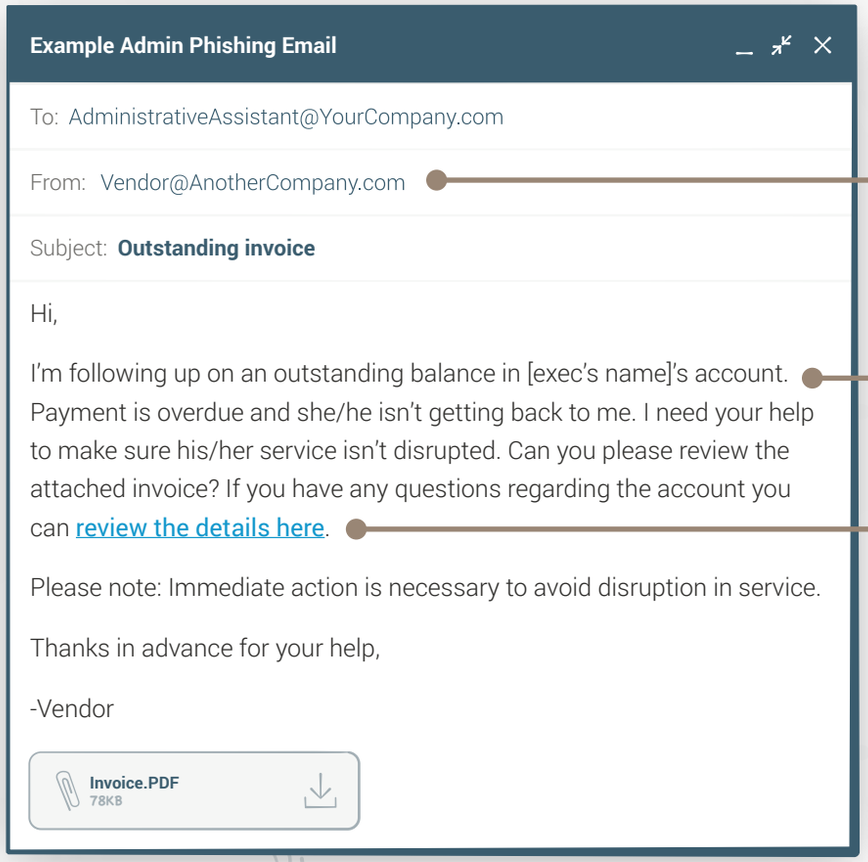
- Provide admin assistants with a clear procedure for how to deal with suspicious emails and report them to IT.
- Make sure you have good email/spam filters in place.
- Limit assistants' access and privileges to the minimum they need to do their jobs.

How to Appeal to Administrative Assistants:

- Assistants tend to be protective of the execs they're reporting to. Leverage that protectiveness by emphasizing it's their job to keep their bosses (and themselves) safe by being on the lookout for phishing attacks.
- Assistants also hate to waste their boss's time. Reassure them being a little proactive now can save time as well as major headaches down the line. Execs would much rather deal with the occasional verification check-in or delay than find out they've been hacked.

What A Phishing Email Might Look Like:

Here's an example of a phishing email an administrative assistant might receive asking them to download and review an unpaid invoice.



Don't download or open attachments from senders you don't know or trust.

Does the executive really have an account with this vendor? Before you respond to any requests you're unsure of, double-check with relevant parties to confirm details and verify they're legit.

The link in the text could go anywhere. Make sure you hover over the link to view the URL. If it looks strange or doesn't match up, don't click.

HABITAT

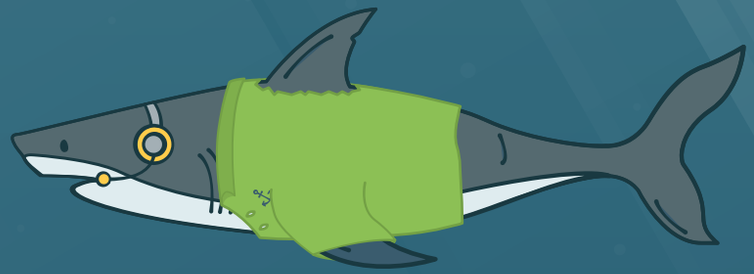
Sales Floor, On The Road, Golf Course

PRIZED FOR

Responsiveness, Email Optimism, Risk Taking

FREQUENCY

Common



The Salesperson

"The Sales Shark"

Alwaysicus Be Closingtatum

Salespeople are the inside salespeople, business development managers, and account executives who are on the hunt for your company's next big deal. They interact with prospective and existing clients in person, over the phone, and via email all day long to drum up new business and keep revenue coming in.

The average day for a salesperson involves a large number of small tasks — making calls, sending quotes, meeting clients, and closing deals. They're always on the lookout for emails from prospective customers. Salespeople want to be attentive and responsive to help close business, so they like to reply quickly to any incoming email or phone call.

Why & How Phishers Target Them:

Salespeople are always chasing the next deal. To them, time is money, and they won't think twice about taking risks and bending the rules if they believe it will help them move faster. They're also prospect-pleasers, and their eagerness to oblige can make them prime phishing targets.

As more and more companies conduct business using digital signatures and online forms, salespeople can easily be convinced to visit an insecure site or download an infected file. By the nature of their jobs they can also be incredibly easy to get a hold of. Phishers can typically find their name, phone number, and email address readily available online, and they can be reasonably confident any message they send a salesperson will be at the very least be opened.

How to Protect Them:

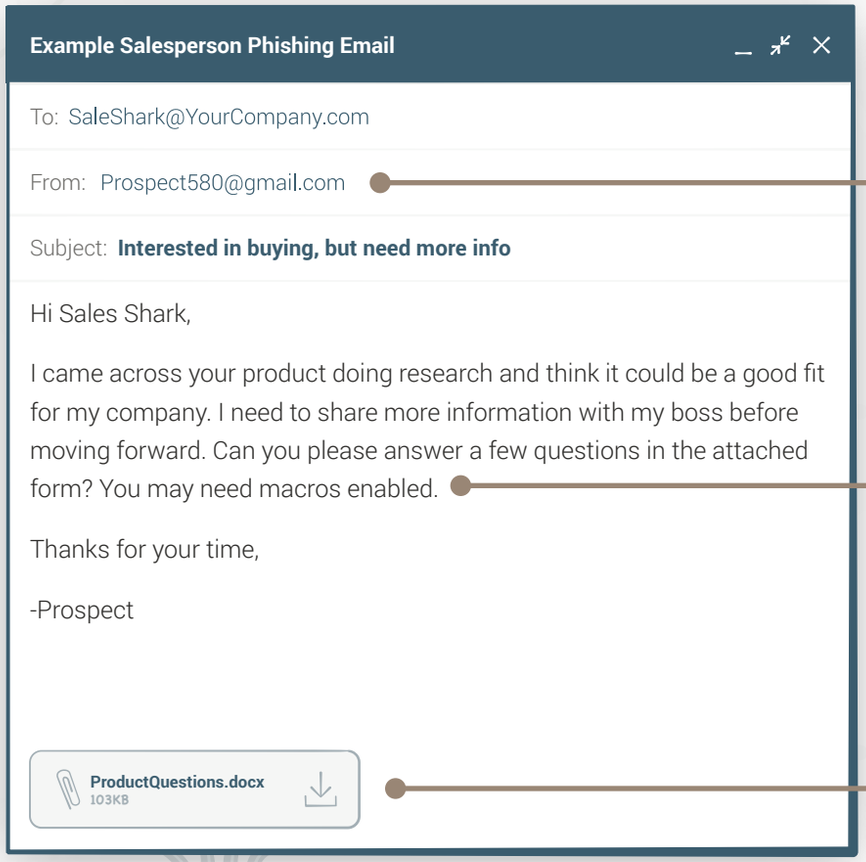
- Talk with your purchasing department about how to transfer POs and invoices through methods other than email.
- Some varieties of ransomware require macros to be enabled. Disable macros across your network to keep a salesperson from accidentally enabling them.
- Remind salespeople to double-check any linked text they receive in an email. Hovering over the link will show them the URL. If it looks sketchy, they shouldn't click.

How to Speak with Salespeople:

- Remind salespeople about the downtime a phishing attack can cost them. If their computer or phone needs to be cleaned and restored that's potentially hours or even days of calls, demoes, and closes they're going to miss out on.
- Salespeople are very concerned with how your company and its products are perceived. Remind them that if they do get compromised by a phishing attack it could severely damage your company's reputation with prospective customers.
- Habit is your best friend when it comes to training salespeople. Breaking down best practices into small, easy-to-follow instructions will help them be more security conscious.

What A Phishing Email Might Look Like:

Here's an example of a phishing email a salesperson might receive asking them to provide product information by filling out a form.



Be wary of professional emails from Gmail, Yahoo, Hotmail or other free email accounts.

Enabling macros for a document you downloaded from an email is a *big* no-no. If you're asked to enable macros when a document opens, close out and delete the file.

Avoid downloading documents or filling out forms when a simple response or an invitation to discuss questions over the phone could suffice.

HABITAT

Interviews, Benefits Meetings, Long Talks

PRIZED FOR

Confidential Info, Tax & Payroll Records, Eagerness to Please

FREQUENCY

Medium

Human Resources

"The Human Resourcetapus"

Benifitus Talkalotis

Human resources professionals are the people people of your company. Their specific roles can vary, but generally they're focused on recruiting and onboarding employees, helping them navigate company policies and procedures, and managing the company's payroll system and benefits programs.

Their jobs require HR professionals to be some of the most highly connected people in your organization. They spend much of their day communicating with current and potential employees, building out their network, and collecting information the company can use to better manage its workforce.

Why & How Phishers Target Them:

By their very nature, members of the HR team are people who like helping others. Their role is often built around sharing information, and they have access to a lot of it. Payroll data, W-2s, employee benefits information, the list goes on.

Phishers can take advantage of this by posing as an employee looking for help accessing their own info, or a high-level executive asking for larger amounts of information. During the 2016 tax season alone, over 50 organizations were tricked into leaking their employees' W-2 forms by phishing emails impersonating requests from CEOs.

How to Protect Them:

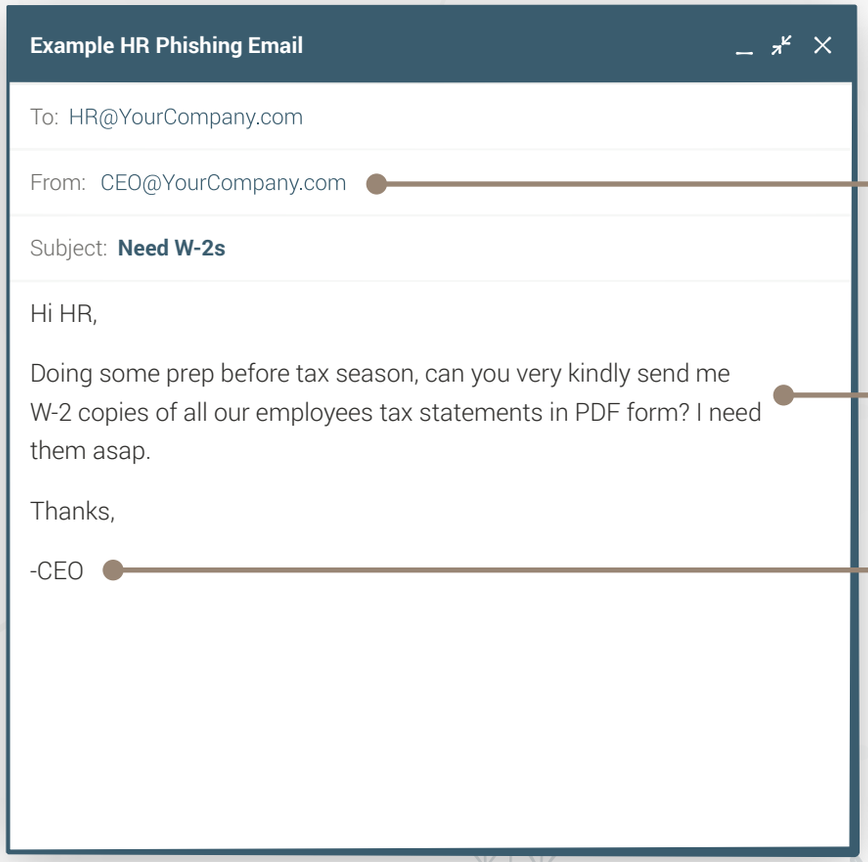
- Invest in benefits software and employee portals so employees never have to send confidential documents over email.
- Remind members of the HR team that any requests they receive from an employee asking for sensitive information should be verified either over the phone or face to face.

How to Huddle Up with HR:

- HR is a job that appeals to people people. Take some time to remind them of the potential harm phishing attacks can cause other team members if they aren't vigilant.
- HR is also a role that appreciates policies and procedures. They're more likely to be receptive to a clear list of things to do and not to do than "Did you know" information about how phishing attacks really work.
- W-2 scam emails targeting HR have been well-documented. Show them real-life examples so they understand phishing isn't theoretical.

What A Phishing Email Might Look Like:

Here's an example of a phishing email purportedly from the CEO asking a HR professional to forward copies of employee W-2 forms.



Be wary of unusual requests, even if they come from the boss. Is the CEO in the habit of requesting W-2 forms? The smart move here is to take a second to verify the request is legit.

Keep an eye out for poor grammar or odd phrasing, which can be a red flag for phishing.

Check to see if there's anything off about the email signature, or if it's missing altogether.

HABITAT

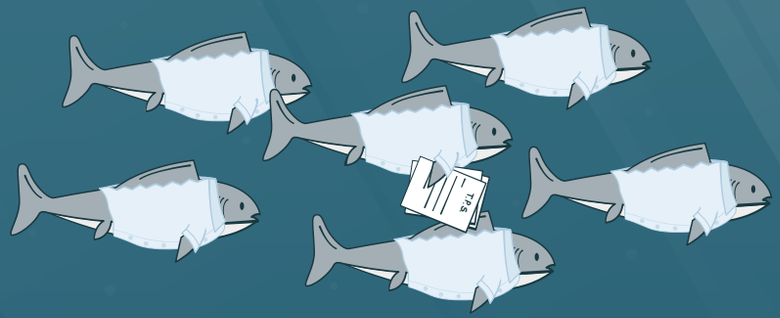
Desks, Offices, Corner Offices, Meeting Rooms, the Water Cooler

PRIZED FOR

Lack of Security Awareness, Travels in Large Groups

FREQUENCY

Common



Every Employee

"The Phisherman's Platter"

Everyoneicus Even Youtum

So far, we've been focused on phishing attacks that target specific employees (what many refer to as "spear phishing" attacks), but the truth is mass phishing attacks are still just as popular as ever.

Before we wrap up, then, here's a quick reminder that anyone at your company — from the CEO to entry-level assistants — can be the subject of a phishing attack. That means your training programs and security measures really need to be addressed to everybody, even other folks in IT. The more people you can get involved (and the easier you can make it for them to get involved), the better.

Why & How Phishers Target Them:

While sending personalized emails to specific targets can be far more convincing and effective, it also takes work, and plenty of attackers still prefer to do things the old fashioned way — send out a generic email blast, and see what casting a wide, indiscriminate net can reel in.

These emails may not be as successful on an individual basis, but with an average success rate of 12% (Verizon DBIR 2016), many criminals are content to simply blast out a high volume of phishing emails and play the odds. After all, it only takes one employee to make a mistake for an attacker to gain access into an organization.

How to Protect Them:

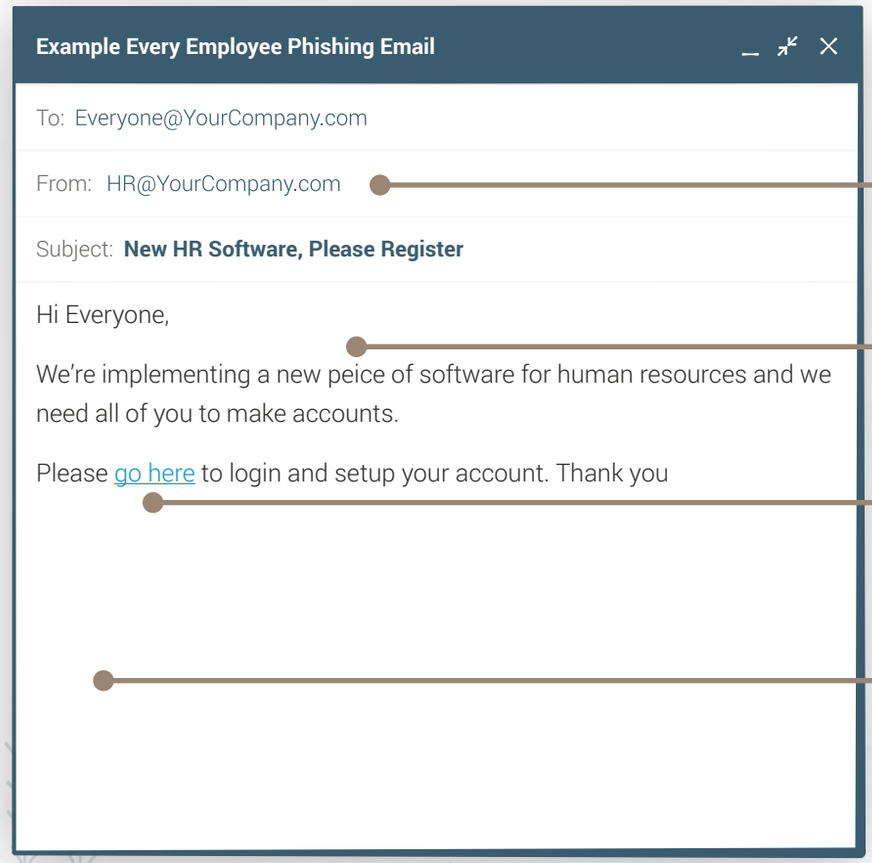
- Utilize spam/email filtering solutions and make sure you have additional endpoint security installed that covers the gaps in antivirus protection.
- Actively encourage employees to contact IT anytime they run across an email that looks suspicious, and provide a clear policy for doing so.
- Make sure you have a company-wide backup strategy and that you're limiting user account privileges.

How to Talk to Any Potential Phish:

- For starters, actually take the time to talk! Get to know what their day-to-day looks like and what their goals and challenges are. Talk about security with those things in mind, and use examples that directly apply to them.
- Give actionable tips, not lectures.
- Make training about helping them (not just the company), and show employees how they can help keep their friends and family safe by being more secure outside of work, too.
- Positive reinforcement works. A company-wide thank-you email praising employees who report suspicious emails can be more powerful than 10 email reminders about not downloading .exe files.

What A Phishing Email Might Look Like:

Here's an example of a mass phishing email posing as an update from HR.



Verify mass emails like this with someone specific. It will only take a second to confirm with someone in HR that this email is legit.

Watch out for spelling and grammatical errors, or any other indications that the tone or style of the email is off.

Check to see where the link is going before you click. Hovering over the hyperlink will show you the destination URL.

Be wary of emails without signatures. Shouldn't an email like this be coming from someone in particular from HR?

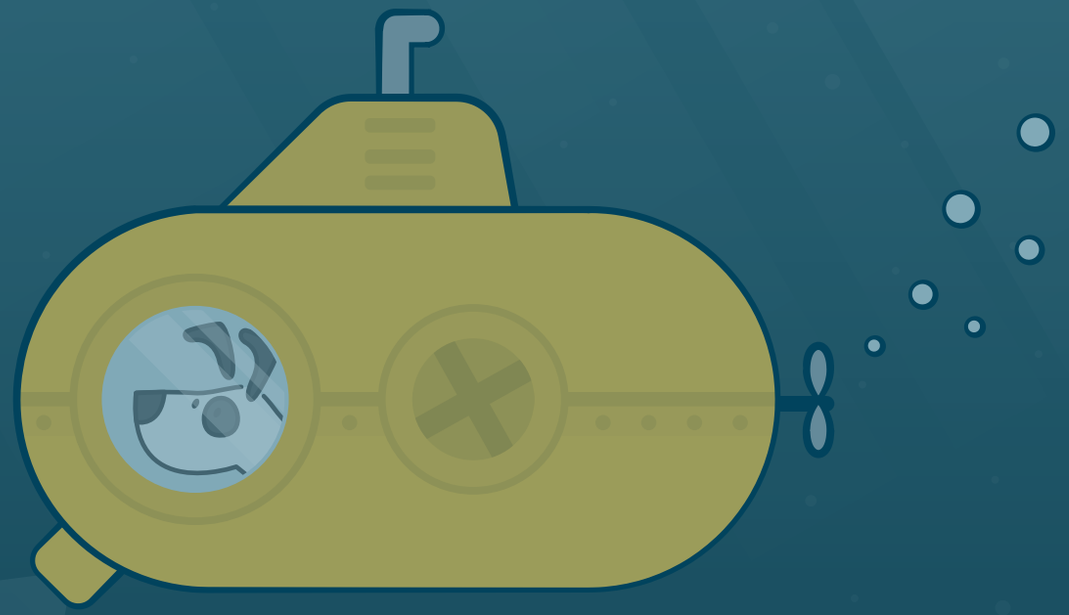
Conclusion

What Should You Do in Addition to User Training?

So, now you've taken a closer look at some of the users swimming in your corporate aquarium (sorry, had to) and learned what makes them valuable and vulnerable from a phisher's perspective. Feel free to print out the sample phishing emails we've provided, along with the bonus checklist at the end of the guide, to help train your users on what to watch out for.

It's important to remember, however, that while user education can do a lot to limit cyber attacks, no training program can guarantee protection from every threat all of the time.

With that in mind, here are some additional steps you should take to protect your organization from phishing attacks and the malware they deliver:



1. Add another layer of endpoint security on top of antivirus

Antivirus solutions are great for blocking malware when they know what blacklisted files to look for, but with more than 390,000 new variations of malware created every day, they have a very hard time keeping up. By looking at system behavior to identify malware instead of matching file signatures, Barkly's new layer of endpoint security stops attacks from doing any damage, even if a phishing attempt is successful.

2. Have a solid backup strategy and test it properly

If you're hit with a cyber attack, especially a ransomware infection, your best bet is to wipe the computer and then restore from your last good backup. That assumes you have a good backup to restore from. To make sure you're prepared, build out a backup that is 3-2-1 compliant — keep three copies of your data in two separate locations, one of which is offsite, and test it at least quarterly. Remember: when it comes to backup you're only as good as your last good snapshot.

3. Let users know what to do if they do have an infection

If you fail to prepare you prepare to fail, especially when it comes to cyber attacks. When you speak to your users about avoiding phishing attacks also remind them what to do if they suspect their machine has been infected: unplug the ethernet cord, shut off the wi-fi, shut down the computer, and report the infection to IT immediately.

4. Disable Office macros

Since a common tactic by cyber criminals is to insert malware through office macros, newer versions of Microsoft Office and Office 365 will enable the IT team to block documents from enabling them. Check to see if your version of Office supports macro blocking and, if possible, adjust your Group Policy settings to disable macros from running.

5. ABP. Always be Patching

Update your software as often as possible and remind your users to do the same. Even better, look into automating patch management and installation.

Appendix

Additional Tools & Resources

Phish your own users with these free phishing tests

KnowBe4
Find out what percentage of your users are "phish-prone" with KnowBe4's free phishing security test.
https://www.knowbe4.com/phishing-security-test-offer

Gophish
Create your own simulated phishing campaigns and track results with this easy-to-use open source platform.
https://getgophish.com/

Anti-spam and email filtering tools

Email Exposure Check (KnowBe4)
Criminals love finding legitimate business email addresses they can use to launch social engineering and spear phishing attacks. Find out how many of your company's email addresses are exposed on the Internet along with where they can be found.
https://www.knowbe4.com/email-exposure-check/

10 Spam Filtering Solutions
The folks at Sitepoint have put together a list of 10 free and paid options that can help you create a spam-free inbox or even stop spam at the server end.
https://www.sitepoint.com/spam-filtering-solutions/

Examples of real-life phishing emails

Phishing Interactive Learning Module (Security Awareness Company)
Give your users the opportunity to see what real examples of phishing emails look like first hand, then test their knowledge by asking them to sort legitimate emails from phishing ones.
http://free.thesecurityawarenesscompany.com/downloads/phishing-ilm/

Several universities also keep online collections of phishing emails their students and faculty have actually received. These are great to share with your users as real-life examples of what to watch out for.

- Cornell University's Phish Bowl
  http://www.it.cornell.edu/security/phishbowl.cfm
- UC Berkeley's Phish Tank
  https://security.berkeley.edu/resources/phishing/phish-tank
- Northeastern University's Phish Tank
  http://www.northeastern.edu/securenu/phishing/the-phish-tank/

Protection for users who do take the bait

Barkly
We don't mean to brag, but our new layer of endpoint security is designed to stop attacks that sneak past users and antivirus. Consider it a safety net you can rely on even when something else slips.
http://www.barkly.com/

Bonus Checklist

5 Tips to Stay Off The Phishing Hook

Always double-check the email address

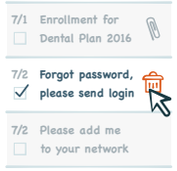
Be on the lookout for any email address that looks funny. Extra numbers at the end, weird domains — if anything makes you think an email might not be from someone you know be sure to alert IT.

Check twice, click once

Make sure you hover over hyperlinks to see the destination URL before you click. Phishers will often hide malicious URLs in routine text like "just click here to confirm." If you hover and the link doesn't match up or looks suspicious, don't click.

Not sure about an email? Check with the sender in person or on the phone

Phishers will often try to impersonate your boss or coworkers to trick you into clicking. If you get an email with any request that seems out of the ordinary — no matter who it's from — call or speak with the sender face-to-face to verify it's legit. If that person tells you they didn't send the email report the issue to IT immediately.



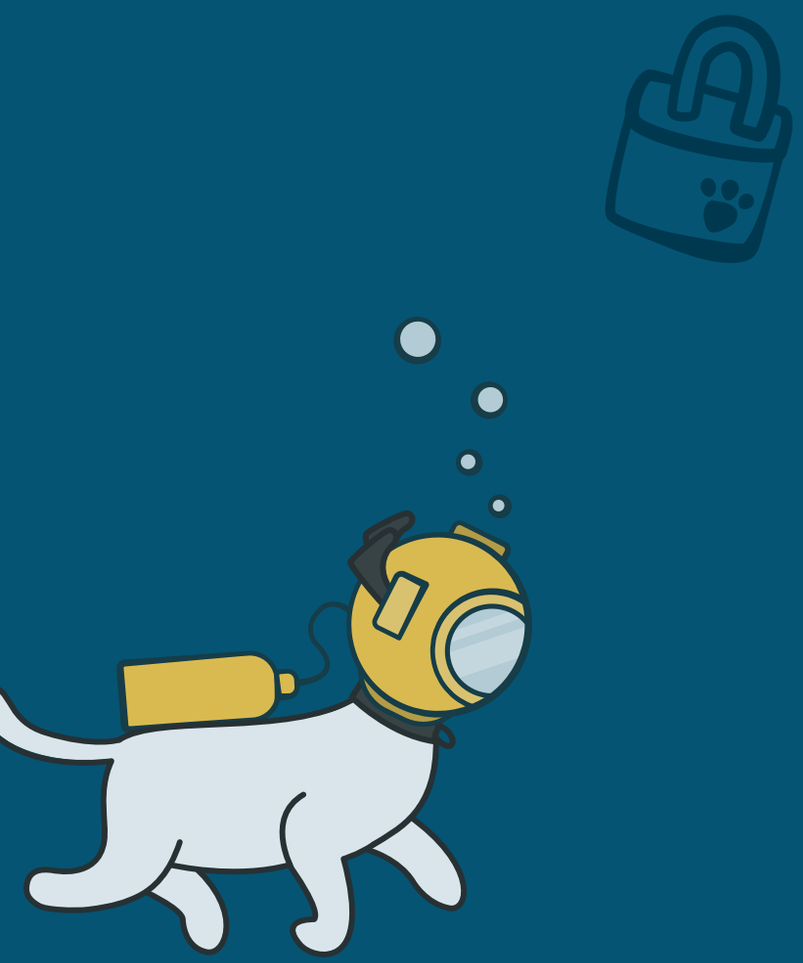
Avoid sending confidential information via email

If you receive an email from anyone asking for sensitive information (your password, W-2s, corporate account information, etc.) play it safe by alerting the IT department. You could be the target of a phishing attack.

Don't enable macros on any attachment

If you receive a Word or Excel file in an email and it asks you enable macros to open it, don't. Some malicious software uses Office macros to activate itself. To avoid getting infected with a virus, ask IT to check out the document first before you open it.

Barkly



Mistakes happen. Barkly is there to protect your users when they do.

Phishing emails are getting more and more convincing. You need something you can count on even if a user does take the bait. That's where Barkly comes in.

We're a new layer of endpoint security that automatically stops attacks before they can do any damage. Instead of scanning files like antivirus and other signature-based solutions, Barkly blocks malware and ransomware by analyzing behavior on end user machines.

See How Barkly Works

Barkly

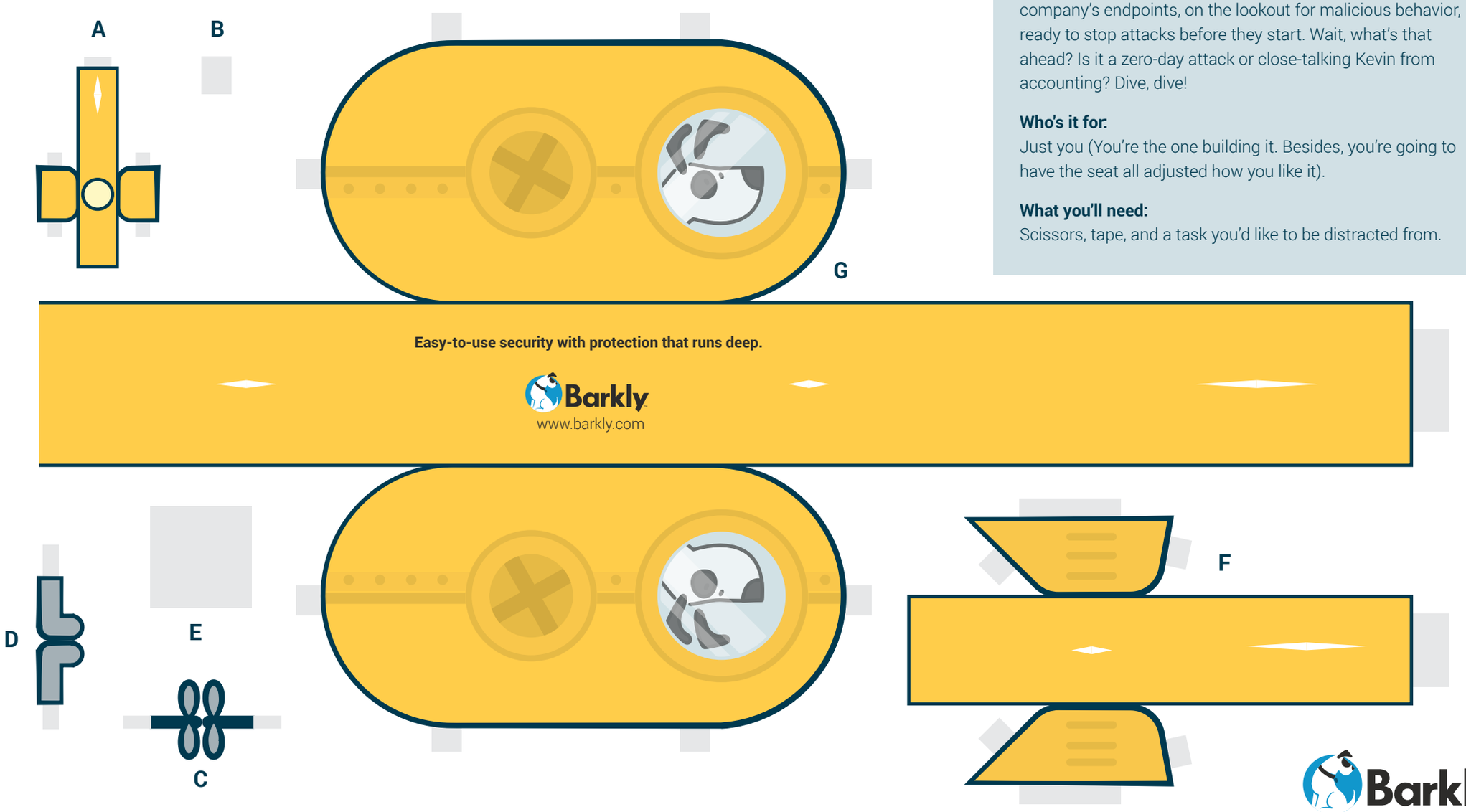
Bonus Prize

Build Your Own Barkly Submarine

What this is:
Go on the hunt for malware with your very own 3D paper Barkly submarine. Imagine you're diving deep into your company's endpoints, on the lookout for malicious behavior, ready to stop attacks before they start. Wait, what's that ahead? Is it a zero-day attack or close-talking Kevin from accounting? Dive, dive!

Who's it for:
Just you (You're the one building it. Besides, you're going to have the seat all adjusted how you like it).

What you'll need:
Scissors, tape, and a task you'd like to be distracted from.



Barkly

Bonus Prize

Build Your Own Barkly Submarine: Instructions

1. **Cut out all pieces and set aside**
   Remember to include the gray tabs, but cut out the diamonds.

2. **Pieces A & B**
   Slide tab (B) halfway through the cutout diamond on (A) and tape to backside of (A).

   Fold the the sides down and use the gray tabs and tape to create the final shape of the light.

3. **Piece C**
   Fold over piece (C) on top of itself. Insert the gray tabs into the rear cutout diamond on the submarine body (G) and tape each tab to the backside in opposing directions.

4. **Pieces D, E & F**
   Fold over piece (D) on top of itself. Insert the gray tabs on (D) into the smaller diamond on (F) and tape each tab to the backside in opposing directions.

   Insert (E) into the larger diamond on (F) and tape to the backside.

   Fold over sides and tape gray tabs to create the final shape of the top of the submarine (F) with telescope (D) and tab (E) halfway out.

5. **Piece G**
   Attach the light (A) to the submarine body (G) using tab (B) and the smallest diamond on (G). Tape (B) to the backside of (G).

   Attach the submarine top (F) to submarine body (G) using tab (E) and the largest diamond on (G). Tape tab (E) to the backside of (G).

   With all attachments on the submarine body (G), fold over sides and tape gray tabs to create the final submarine body (G).