

**Phishing attacks  
are responsible  
for more  
than 80% of  
reported security  
incidents.<sup>1</sup>**

## The Headlines

### **"Ukraine and US Targeted by Cybersecurity Attacks in Run-Up to Russian Invasion"**

Google's Threat Analysis Group (TAG) has observed activity, ranging from espionage to phishing campaigns, from threat actors, including FancyBear and Ghostwriter.

### **"New IRS Rule Will Lead to Widespread Phishing Scams"**

Though the measure is to cross-check taxable income...those receiving payments for goods and services rendered through online payment services will be asked for their social security number or tax ID and other private data.

### **"Brunswick County Loses \$4 Million in Email Phishing Scheme"**

The USSS Wilmington North Carolina Resident Office (RO) was advised by the Brunswick County Sheriff's Office that the County had been affected by a business email compromise (BEC) and suffered a total estimated loss of \$4,026,180.07.

## The Situation

Ah, phishing. Strange to think that its homophone – fishing – is such a relaxing pastime, when "phishing" can strike terror into the heart of anyone with an email address.

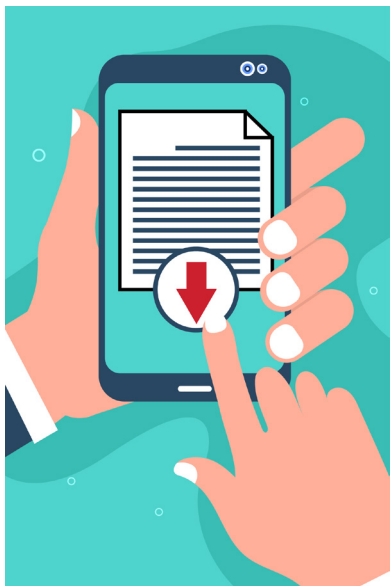
Phishing (which probably doesn't need to be defined anymore, but we will anyway) is when an adversary tricks an email recipient into revealing sensitive/personal information. The recipient believes the message is from a legitimate source and clicks on a link, downloads an attachment, or types their credentials into a faux website page. Then, all hell breaks loose, i.e., ransomware, malware, etc.

Almost all phishing attacks start with social engineering. The most basic definition of which is: Deceiving or manipulating people via email, text, social media, or phone call to gain access to confidential information for fraudulent purposes. By getting to know their victims – names, job titles, even favorite websites – through a little online research, adversaries have a much better chance of getting their targets to do exactly what they want.

### Types of Phishing

Cybercriminals are always developing new techniques to dupe people into giving up their personal information. Below are a few of the tried-and-true methods adversaries use most frequently.

- **Email/spam** – The most well-known type of phishing, this type is sent to millions of people and typically includes an "urgent"



**"Spear phishing only works when the misleading email content is relevant to the recipient."**

-Stu Sjouwerman,  
KnowBe4

message in the hopes that recipients will download a file or click a link that sends them to a malicious website that requests personal info or installs malware without the user's knowledge.

- **Spear phishing** – A more targeted approach, adversaries gather info about a company – such as employee names and job functions, telephone numbers, and other data – to make their emails sound more legitimate and thus more likely to succeed.
- **Business email compromise** – A BEC is when an adversary successfully compromises an email account through credential harvesting (getting a user to enter username and password into a bogus login page). Once in, the bad actor impersonates the user, tricking more people to fall for the same attack; changes rule sets within the mailbox to avoid detection; and intercepts transactions of personal or financial data. (Read the [blog article about BECs](#) by our Director of Cybersecurity Operations, Brandy Griffin.)
- **Whaling/CEO fraud** – This type of BEC is directed at the "big fish" in a company to lure them into taking the bait, i.e., clicking on a bad link or attachment or transferring large sums of money.
- **Vishing (voice phishing)** – An example of this is the infamous IRS call during tax season, which threatens an audit and "requires" the victim to provide personal information like a social security number.
- **Smishing (Short Message Service [SMS] phishing)** – Examples of smishing include a mobile text that indicates an Amazon order has been delivered or that your bank account has been hacked, and provides a link to a malicious website.
- **Angler phishing** – This type of phishing uses social media notifications and messages to persuade someone to take action, such as providing sensitive information or credentials.
- **Watering hole phishing** – Adversaries learn which websites a company's employees visit frequently, such as a third-party vendor, where they look for vulnerabilities that will allow them to inject malicious code into that site. An employee then visits this "trusted" site and unwittingly downloads malware, which infects the user's computer.



**495 million  
ransomware  
attempts took  
place in the first  
nine months  
of 2021.<sup>2</sup>**

## BECs: Laws, Regulations, and Penalties

While business email compromises are sadly an everyday occurrence, they can be addressed with proper implementation and management of security controls (see both “Solutions” sections). Yet somehow, these types of cyber incidents continue to happen, which is why state and federal agencies are becoming more stringent with organizations that fail to take proactive security steps.

An example of this is a mortgage company that failed to disclose a BEC, which resulted in a [\\$1.5 million penalty](#). Another case identified a life insurance company’s failure to implement multi-factor authentication, which ultimately led to successful malicious email phishing attacks compromising several email mailboxes containing sensitive information; the insurance company was [fined \\$1.8 million](#) for their non-compliance and the consequential outcome.

The Securities and Exchange Commission also [fined multiple firms](#) due to lax cybersecurity policies and controls, which resulted in numerous email account takeovers exposing thousands of consumers personally identifiable information (PII) records. It’s easy to see that these fines will continue to mount until organizations of all sizes take security seriously.

## Ransomware

One of the biggest concerns related to phishing attacks is ransomware. And with good reason. According to SonicWall, [495 million ransomware attempts](#) took place in the first nine months of 2021. In 2020, there were 304.6 million attacks for the entire year. Overall, ransomware has risen a mind-blowing [231.7% since 2019](#).

Phishing emails are a relatively easy way for cybercriminals to deploy ransomware, as you only need one person to open an email and click on a malicious link or attachment, thus allowing the adversary to take over the victim’s computer. That person’s files are then encrypted and cannot be accessed until the ransom is paid.

Read more about ransomware, in particular, whether or not you should pay the ransom, at our [blog](#).

**"Security awareness can help minimize some of the business risks organizations face with social engineering attacks."**

**Kyle Cavalieri**  
President,  
Avalon Cyber

## If an Employee Clicks a Phishing Link

Don't panic, but don't ignore it either. Due diligence is always warranted in the face of a suspected cyber incident. Have your IT department or managed security service provider (MSSP) determine whether the phishing attempt was successful. If they identify unusual artefacts or behavioral characteristics, contact legal counsel and your cyber insurance provider, and follow these steps:

- **Contain the incident** – Your IT team can blacklist the sender's profile and, depending on the email platform, should be able to search for and delete all known phishing emails from users' mailboxes to stop others from falling prey to the attack.
- **Change your passwords** – Be sure everyone impacted changes their email account passwords – you may even consider a forced global password change across your organization – and implement multi-factor authentication (MFA) if you haven't already. [See "Solutions You Can Implement Right Now"]
- **Launch a more comprehensive forensic investigation** – Your cyber insurance company will help bring in the right people, including legal counsel (if you don't already have your own) to navigate the legal implications of the incident and a third-party [incident response team](#), such as Avalon Cyber, to identify the source and extent of the incident, and minimize damage (if any) to your IT environment. Through their forensic investigation, your IR team will determine the scope of the incident, which will lead to a plan of action to remediate the issue at hand and provide a set of "lessons learned" to help prevent future attacks.

## Three Questions a Forensic Investigation Seeks to Answer

1. **How did the attackers get in?** Determine the cause of the incident and how and when it occurred.
2. **Where did they go?** Whether the attacker stays in the email environment or moves into your network, they will likely attempt to obtain additional credentials from users or administrator accounts. If they gain sufficient access, an adversary can also create accounts for later use within your environment.



Use a **password manager** to ensure that your employees **create strong passwords**, but **don't have to remember them**.

3. **What did they take?** Verify whether sensitive information, such as personally identifiable information (PII), protected health information (PHI), and/or proprietary information, was accessed or exfiltrated, and which businesses and individuals were affected. This may require you to provide breach notifications to impacted entities.

## The Solutions You Can Implement Right Now

A few tactics to employ at your company to reduce the risk of a business email compromise include:

- **Utilize multifactor authentication (MFA)** – Before you [move to MFA](#), prepare your team. By explaining the need (it will protect the company as well as each employee), and taking the time to train and educate, the transition will be more readily accepted, and productivity will remain stable. Avalon Cyber recommends authentication apps, such as Duo Mobile, over text messages for purposes of MFA due to the rise in [SIM-swapping attacks](#).
- **Enforce strong password policies** – Configure password settings to require longer, more complex passwords across your network and all business applications. While there are various recommendations based on security frameworks, Avalon Cyber suggests that passwords be at least 15 characters with a mix of letters, numbers, and symbols. (See how fast a cybercriminal can crack your password in the graphic on the following page.) Use a password manager (i.e., LastPass, DashLane, etc.) secured with a master password and MFA to ensure that your employees create strong passwords, but don't have to remember them, as the software automatically enters and stores passwords for them.

As mentioned earlier, phishing attacks can lead to ransomware. Here are a few ways to reduce that risk:

- **Keep your operating systems and software updated** – Be sure to apply updates whenever they're released.
- **Whitelist safe applications** – By generating an index of approved software applications or executable files, you help limit the chance of an attacker running malicious programs on your system.
- **Develop network diagrams** – A diagram of all the devices





The **average organization** is targeted by over **700 social engineering attacks** each year.<sup>3</sup>

on your network – from hosts to routers to access points – will provide your IT and security teams with a better understanding of what systems connect to each other and help them identify the potential spread of malware.

- **Create, update, segregate, and protect backups** – A reliable data backup may prevent excessive damage to your information in the event of a ransomware attack, as your data will be stored safe and sound outside your network.
- **Block legacy authentication (POP3/SMTP/IMAP/MAPI)** – Doing this prevents credential exposure due to outdated protocols and ensures MFA cannot be bypassed, as legacy authentication cannot enforce MFA.
- **Have a plan** – This one is obvious, but unfortunately, many companies don't have a cyber incident response plan in place. Which brings us to the next section in which we discuss the many ways Avalon Cyber can help protect your enterprise from all types of cyberattacks.

## TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	1 sec	5 secs
7	Instantly	Instantly	25 secs	1 min	6 mins
8	Instantly	5 secs	22 mins	1 hour	8 hours
9	Instantly	2 mins	19 hours	3 days	3 weeks
10	Instantly	58 mins	1 month	7 months	5 years
11	2 secs	1 day	5 years	41 years	400 years
12	25 secs	3 weeks	300 years	2k years	34k years
13	4 mins	1 year	16k years	100k years	2m years
14	41 mins	51 years	800k years	9m years	200m years
15	6 hours	1k years	43m years	600m years	15 bn years
16	2 days	34k years	2bn years	37bn years	1tn years
17	4 weeks	800k years	100bn years	2tn years	93tn years
18	9 months	23m years	6tn years	100 tn years	7qd years

Source: Hive Systems



-Data sourced from [HowSecureisMyPassword.net](https://HowSecureisMyPassword.net)

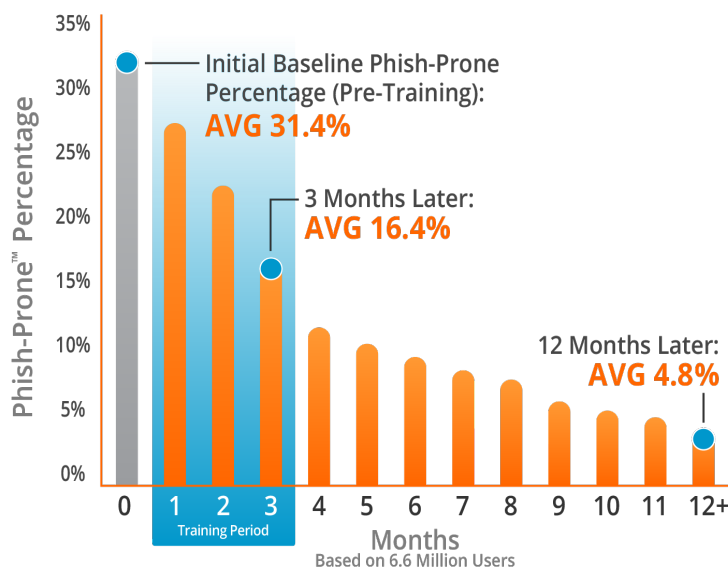
## The Solutions Avalon Cyber Can Provide

While putting the solutions listed above into effect will help protect you from falling victim to phishing scams, as well as ransomware attacks, it's always best to get professionals involved in your cybersecurity strategy. Avalon Cyber offers a complete range of proactive and reactive services to help you achieve a greater level of data security.

### Phishing Simulation & Training

No matter what size your business, [training your team](#) to recognize phishing attempts is a crucial addition to your security plan. Get them to think of emails as weapons because in the cyber world, they are. You want everyone from your C-suite to part-time workers to vendors on the same page when it comes to phishing and security.

Here's how  
successful  
training and  
testing your team  
can be:



Avalon Cyber and our partner KnowBe4, the world's largest security awareness training and simulated phishing platform, offer an innovative program that allows your security team to launch best-in-class, fully automated simulated phishing attacks and run comprehensive security awareness training campaigns to help educate your employees and stakeholders.

It's important to run these tests and training programs regularly to keep security top of mind and to test using the most up-to-date phishing attack methods. We even offer a [free phishing security test](#) if you'd like to see how your company fares against phishing lures.



If you **experience**  
**a cyber incident**,  
it's critical that  
you **quickly**  
**find and fill the**  
**gap in your**  
**network** and  
identify what data  
may have been  
compromised.

## Vulnerability Assessments

Avalon Cyber's expert engineers conduct internal and/or external scans to [identify vulnerabilities](#) and basic misconfigurations in your company's environment. Our team provides a comprehensive report and works with you every step of the way to develop a plan to address the most critical weaknesses and provide insights into the best way to implement improvements.

## Penetration Tests

Our cybersecurity professionals safely simulate the actions of a cybercriminal targeting your network and attempt to exploit critical systems to access sensitive data. [Penetration testing](#) validates the efficiency of your currently deployed security resources and determines how well IT teams are implementing controls and whether employees are following existing security policies.

## Managed Detection and Response (MDR)

Our [KnightVision MDR](#) service is a robust endpoint monitoring solution that screens malicious behavior at the endpoint level, allowing our team of experts to alert you and take immediate action to shut down a potential threat.

## Incident Response

If you experience a cyber incident, it's critical that you quickly find and fill the gaps in your network and identify what data may have been compromised. This process is a true forensic analysis process that traditional IT companies don't necessarily have the capacity for. The Avalon Cyber team has extensive experience in digital forensics and [incident response](#) and provide prompt and comprehensive response to cyberattacks. Our experts know where to find critical electronic evidence, and concurrently preserve and analyze it using today's most sophisticated digital forensic techniques and software. Avalon Cyber also offers assistance with [data breach review](#) and [data breach notifications](#).

## SIEM and Managed SOC

Our [KnightVision CAM](#) (which stands for Compliance, Alerting, and Monitoring) combines a Security Information and Event Management (SIEM) platform, which collects, aggregates, and analyzes security





For immediate  
assistance, call  
**Avalon Cyber's  
Incident Response  
Team at:  
877.216.2511**

event log data, and a managed Security Operations Center (SOC), i.e., a team of cybersecurity experts who respond to detected threats immediately. It's Avalon Cyber's customizable, scalable, affordable solution that addresses a range of cybersecurity challenges, including regulatory compliance, threat detection, and incident response.


## Incident Response (IR) Planning

Just as you run fire drills to keep your employees safe, your company should also practice managing security breaches together. Avalon Cyber's [incident response planning](#) service helps you identify, protect against, detect, respond to, and recover from a cyber incident. Our team can guide you through plan creation and tabletop exercises, in which we run through various threat scenarios and practice how you would respond to those threats. We can also help you implement tools and technology to manage and mitigate security incidents. Remember, since threats constantly change, your IR plan will need to be modified and tested regularly. To further assist you, we offer an [IR retainer program](#) that allows you to have a cyber team on call 24/7/365.

## Security Advisory Services

Avalon Cyber team members are highly experienced cybersecurity strategists, and follow an approach founded in our industry experiences from both commercial and military sectors. We blend practices from Big 4 audit and consulting firms, as well as Department of Defense information assurance programs. Our deep understanding of governance, risk management, and compliance allow us to help you build a highly resilient cyber program, while simultaneously enabling productivity and the continued success of your business. Our [advisory services](#) include policy and documentation development, readiness assessments, and IT risk assessments.

## vCISO

In this type of engagement, Avalon Cyber steps into the role of a [virtual chief information security officer \(vCISO\)](#) for companies that do not have the need or means to hire and pay for a full-time resource. Typically, this hybrid approach includes a few hours every month in which our experts become an extension of your team and provide support by overseeing the design, development, and integration of your cybersecurity program. 

<sup>1</sup><https://spanning.com/blog/cyberattacks-2021-phishing-ransomware-data-breach-statistics/>

<sup>2</sup><https://www.sonicwall.com/news/sonicwall-the-year-of-ransomware-continues-with-unprecedented-late-summer-surge/>

<sup>3</sup><https://www.zdnet.com/article/average-organization-targeted-by-over-700-social-engineering-attacks-each-year-report/>



Don't miss out on  
more free content  
from Team Avalon!

Join the Avalon mailing list  
to receive useful  
case studies, industry  
insights, handy tips, and  
more delivered straight  
to your inbox.

[Sign up to receive  
exclusive content!](#)

## About Avalon Cyber

With decades of experience in the domains of digital forensics, cybersecurity incident response, IT risk management, and enterprise information security leadership, Avalon Cyber is the premier solution provider for cybersecurity and incident response services. Our business was built on principles and sound ethics, acquired through years spent working in law enforcement, that can be relied upon and trusted.

Our professionals have been conducting digital forensic and cyber incident response engagements since the early 2000s and have a deep understanding of adversary behaviors and their ever-evolving tools, tactics, and techniques used to compromise networks. The team members who support our managed security services have extensive experience in information security, have or previously have held top secret government clearances, and possess key industry certifications including: CISSP, OSCP, GPEN, CISM, CISA, CCNA, CCE, CFCE, EnCE, ACE, GXPEN, OSCE, GSEC, ECIH, SSCP, CCSFP, and SEC+.

Avalon Cyber works for organizations looking to partner with experts to achieve a greater level of data security.

## QUESTIONS?

For more information on any of our services,  
please contact:

**Ian Gattie**

Director of Marketing

[ian.gattie@teamavalon.com](mailto:ian.gattie@teamavalon.com)