CHRIS'LL DEAL WITH IT episode notes

EP 52 - Grandma's Wishing Nobody's Phishing

Status	Published ✨
Publication Date	@January 14, 2024

🎙️ **www.ChrisKreuter.com/CDWI**

© 2024 by Kreuter Studios - All rights reserved

🤖 *AI Statement: All elements of this episode are products of the author, Chris Kreuter, made without any use of AI tools.*

Today's Question:

> *My mother-in-law recently reacted to a shady text message that was a clear phishing attempt. We cancelled her credit card in time, but I worry this won't be the last time, because she's not great with tech. Do you have any advice on how I can help her better recognize and understand these threats, while also limiting her exposure to them?*

Phishing *- A form of social engineering where a cyber threat actor poses as a trustworthy colleague, friend, or organization. Their goal is luring out sensitive information or network access. Lures can include emails, text messages, or even phone calls. If successful, they can gain access to more than just the target's information. It* *could be access to a larger network, organizations they're part of, and future third party targets. Victims can experience data or service loss, identity fraud, malware infection, ransomware, monetary loss, impacted reputation, and more.*

Statistics

- Phishing is the most common form of cyber crime. Many estimates say between 80-90% of cyber crime is though a phishing attack.
- The FTC (Federal Trade Commission) reported consumers lost nearly $8.8 BILLION to scams in 2022 alone. An increase of over 30% over 2021.
    - Of this: $1.2 billion through social media!
    - And this isn't even a complete picture, as only 23 states report into the FTC's Consumer Sentinel Network!!!
    - *This is despite the active cyber security measures employed by the massive corporations responsible for delivering much of our digital existence!*
    - Google blocks around 100 million phishing emails every day!
- We regularly hear about data breaches in the news.
    - These are common ways of exposing contact info (e-mails, phone numbers, addresses) that then enable phishing attacks.
    - Leaked or hacked e-mails provide cyber attackers with powerful templates. They use these to build realistic spoofs to trick additional targets.
    - I've seen this first hand with devastating effectiveness. Some of these attacks are very sophisticated.
- It's common for bad actors to imitate brands many of us use. Commonly spoofed brands include:
    - Shipping companies: DHL, FedEx, UPS, and even the US Postal Service
    - Google
    - Microsoft
    - Amazon
    - LinkedIn

- This is a global problem across all industries and countries
- Given our asker's question, it's important to note that the elderly are not the worst actors here.
    - 18-40 year-olds are just as susceptible as senior citizens!
    - Sometimes more so as they are publicly online more, and in more places, creating more 'spoofable' content.

Let's tackle this question in five phases:

P - Provide Perspective

H - Help Genuinely

I - Introduce Better Tools

S - Setup Safeguards

H - Heed Rules

P - Provide Perspective

- What methods do phishing attacks use?
    - text messages
    - e-mails
    - phone calls
    - social media
    - look-alike/imposter websites
    - the most intense scams combine these methods to immerse targets into a faked situation
- What types of scams are there?
    - Corporate Imposters

  - Online shopping (delivery issues, negative balance, even claims of fraud can be fraud)
  - Prizes, sweepstakes, lotteries
  - Investment opportunities (including MLM or Multi-Level Marketing scams)
  - Business & job opportunities
  - Charity scams
  - Romance scams
- How do scammers actually get your money and/or information?
  - Bank/Wire Transfers (this can include making changes in account information to affect transactions to occur later)
  - Direct account access (logging into your account and changing credentials, locking you out as they transfer funds directly)
  - Credit Card account numbers (tends to be abused quickly, spamming businesses local to you, getting whatever they can before the card is either reported or shut off for fraud)
  - Payment Apps (Cash App, Venmo, Paypal, Zelle, etc…)
  - Gift Cards (pleas for help with shopping, assisting with someone's financial loss. Remember that gift cards are not safe assets: Use them as quickly as you can!)
  - Cryptocurrency (nearly impossible-to-trace, digital assets that quickly disappear)
  - Using stolen identities to mimic you in other places (opening fake accounts, taking out loans, stealing social security benefits & more!)
- Where can phishing attacks occur?
  - At home
  - At work (Where they can undermine an entire business, impacting co-workers, customers, and vendors.)
  - Clubs, groups & other recreational organizations

    - Without your involvement at all, if your information was exposed through the victimization of a friend, family member, or corporation that has your sensitive info.
- How bad will this situation get? **A lot worse.**
    - AI voice mimicking is getting close to life-like
    - AI video spoofing as well: Many social media scams leverage this right now, thanks to a combination of virality, algorithms, and a lack of education & desire to vet the legitimacy of information.
    - The use of social engineering: Emotional pleas, realistic scenarios, and intense details that build trust and/or create a sense of urgency - These can trigger victims into quick action with less discernment.
    - These are becoming increasingly sophisticated and ruthless attacks. A single scam can ruin a family, no matter how smart, well educated, and intentioned they are.
    - The aims of bad actors are not always financial: Phishing for information can lead to revealing sensitive details that can aid physical attacks and/or terrorist activities!

H - Help Genuinely

- A lot has changed with technology over my forty-plus years.
    - During the 1980's, I had a mostly analog childhood. Households were starting to get online, experimenting with phone line modems and internet service providers like Prodigy & America Online.
    - By the time I entered college, the internet was a major force in society. Corporate and government systems were managing themselves online - and many others were going through the process.
    - Before I turned thirty, social media exploded in use: MySpace led to Facebook, LinkedIn, Instagram, and the many others. This was happening in large part to the development of smartphones around 2007. With many of us getting computers in our pockets, our culture shifted to an always-on mentality.

    - And now in my fourth decade, we're seeing massive developments & investments in algorithms, automation, and artificial intelligence. The human costs to produce scams are nearing zero, which is why we're seeing significant upticks in the quantity and quality of cyber scams.

- Now imagine you were in your parent's shoes:
    - There were still major technological & societal shifts, such as the growth of television, the space race, and suburban expansion, just to name a few.
    - But the impact of these changes on day-to-day life were lower and slower.
    - The overall complexity of the tools embedded in their daily lives was lower than it is today.
    - And there were far fewer ways these new technologies enabled fraud against unsuspecting people.
- Therefore, it's important to accept where they're at.
    - Everyone has a different ability to grasp the information and techniques you'll be trying to convey.
    - Remember that the *<u>pace</u>* of change far exceeds what they grew up with.
    - You likely grew up surrounded by digital technology - they didn't
    - All these threats can be scary… their experience of the world is more analog - and there's a likelihood many of the terms and inner workings of the technologies are difficult to understand.
    - However, in our modern society it is very difficult to NOT be online - Many government agencies, corporations, and even small businesses require online components, interaction through chat-bots, QR codes, apps, reward programs, and online accounts with logins and passwords.
        - I have over 200 logins in my password vault! Even I'm overdue for some internet spring cleaning.
    - All of this online presence is done under the guise (and to some extent the reality) of convenience.
- **Each interaction online does come with some risk: Remind them that everyone has a responsibility to pay attention to the issue. Ignorance is no**

longer permissible!

  - It’s better to ask for help in protecting themselves now rather than begging for forgiveness and/or restitution later

- Getting frustrated with them will be perceived as an indictment on their intelligence.
  - Keep reminding yourself of your best intention: To be genuinely helpful in protecting your parent/in-law and those around them.
  - Don’t talk down to them.
- This is going to require persistent effort: It’s not something that will be solved in one sitting or with a few quick fixes.
  - It will take everyone’s constant vigilance - and a continuing education into scammers’ strategies and tactics

I - Introduce Better Tools

- Have them rethink their need for a smart phone. This is definitely on a case by case basis - as there are are legitimate needs for these powerful devices.
  - If our askers’ family member predominately uses their phone for calls, text messages, and messaging applications - a modern “dumbphone” may be a much better option
  - This would force activities such as online shopping, web browsing, and social media engagement to occur on a regular computer - which offer better navigation, customization, and firewall protections.
  - These larger screens also allow for magnification of text and images, making it easier for elderly people with poor eyesight.
- Ensure they’re registered for the National Do Not Call Registry. While many would agree there are mixed results, regulators such as the FTC are making efforts to curb robo-calling and cold marketing calls.
  - The best way to take advantage of their efforts is to at least be on the registry list.
  - The website for the registry also contains the form to report unwanted calls, which helps with their enforcement efforts.

- Review all of their subscription services
    - For services they want & consistently use: Consider turning them from monthly auto-renewals to annual one-time payments.
    - This has 2 major benefits:
        - A one-time annual commitment often offers a cost savings.
          For example: The current one-time yearly subscription rate for Amazon Prime costs $139 per year, as opposed to $15 per month (a $41 savings!)
        - Re-upping every year can be done as a one-time payment, rather than using a stored card on the Amazon website.
- Which brings us to saving credit/debit card numbers or bank account information on websites and online portals This includes online shopping, utility payments, and medical portals. Each one of these is a potential vulnerability to a bad actor. All for the benefit of the removal of a small amount of friction.
    - Many credit card companies will provide a service to create virtual credit card numbers for temporary one-time purchases, or even repeat purchases from the same source, such as a subscription. They'll also allow you to setup an expiry date.
    - Many utility bills can be paid as they come in using online, one-time payment portals without having to login and save payment information.
    - They'll need a system to remember which bills need these methods, but don't forget that most people over the age of forty grew up learning how to balance a checkbook. They'll likely get used to doing things "a little more old school" quicker than you would.
- Use a VPN service
    - Avoid submitting/sharing sensitive information (especially card #'s and banking info) over public wi-fi or on a public computer (such as at a library).
    - Packet sniffing by bad actors can occur in physical locations such as coffee shops or co-working spaces.
    - Their internet service providers are also mining tons of data from their internet use.

    - These threats can all be easily countered by using a VPN (Virtual Private Network) service. There are many reputable ones out there that offer excellent protection for modest fees and minimal impact on your internet bandwidth.
    - But this additional complexity and steps before getting online may be a bridge too far. Finding ways for a VPN service to enable right on computer start-up would be the best way to go.
- Research companies and charities before taking action.
    - Do official websites or watchdog groups list the same contact information, domain addresses, and content as the suspected scam?
- Avoid sites and services that can be rife with scams or potential for abuse, such as: Craigslist and Facebook Marketplace!
    - Using these sites can lead to situations with real physical danger.
    - Make no mistake that bad actors are praying on people through these convenient, more locally-oriented services.
- Consider a password management system.
    - Every site or system should have a unique password associated with it.
    - With so many passwords they can be difficult to remember
    - Avoid using the same password for everything
    - Avoid easily guessed passwords, especially those tied to publicly-available information such as: Names of family members, dates of birth, model of car, breed of pet, street address, places of education/worship, etc…
    - The length of a password often matters more than complexity. It’s okay to use a series of longer, unrelated words that could make it easier to type & remember.
- And lastly, add a passcode to their mobile device!

S - Setup Safeguards

- **Never share account information, credit card information, passwords, banking details, or sensitive personal information with anyone who contacts you over text, phone, or e-mail.**

- Confirm anyone claiming to be a representative is really who they say they are.
    - When in doubt: Hang up, locate the company's customer support hotline, and redial that number.
- If possible, setup 2-factor authentication for them if it's possible.
    - This is where a website will text or e-mail you when logging in online with a password to confirm the login is authentic.
    - Some might offer setting up a PIN number in addition to a password.
    - Text is preferable to e-mail (different device)
- Create a safe word for family members - and don't share it!
    - Alternatively, if you suspect someone is mimicking a family member, ask them an unusual question from your shared past. One that's obscure, but easily answerable by that family member.
    - Real-life example: If I get a strange call from my sister, I might ask: *"What made me give you the phone when we were kids?"* If she doesn't answer quickly with something like, "*threaten you with a knife*", I know it's a scam. There's no way a phisher would know this off the top of their head! *(Until now, I suppose)*
- Avoid shared accounts
    - This includes setting up a way for your parents to use your accounts, thinking it's easier for you to monitor.
    - You may be reducing the number of targets, but you're making the remaining targets bigger.
- Try to limit interactions on communication apps such as WhatsApp and Facebook Messenger that are highly susceptible to scams & phishing attacks.
    - At the very least NEVER put any sensitive information into those chats.
    - If someone gets access to your account, those direct messages can be create more problems.
- Don't let grandkids be on their phone! They might click a random phishing text pop-up that comes into the device, or accidentally (or on purpose) look through your e-mails and click a malware link.

    - If you absolutely have to have them use an app for something, teach your in-law to at least put their phone into airplane mode first.
- Perform regular bank statement checks - monthly if on paper. Weekly if they have online banking access.
- Have them regularly change their credit card #.
    - This may seem like an annoyance and hassle, but it can help reduce the risk of exposed numbers from third party breaches
    - It also helps prevent continued monthly charges for accounts they're not using, forcing them to reconfirm their subscriptions, with some potential money savings as an added bonus.
- Properly remove all personal data before donating, recycling, or trading in old, damaged, or non-functional devices (tablets, cell phones, laptops, etc…)
- Secure and properly destroy physical documents with sensitive information
    - Examples: Utility bills, credit card offers, bank and investment account statements…
    - Be cautious in your definition: No harm in shredding more than necessary!
    - Some towns offer free periodic shredding programs - but many office supply stores offer reputable and secure shredding services for modest by-the-pound fees.
- Utilize e-mail spam filters
    - If they're using old, badly protected mail clients like AOL - have them setup new accounts
- Have them check if they have identity protection insurance through an employer or other insurance program. Or have them purchase supplemental protection.
- Go Old School!
    - Using checks is still legal and accepted in more places than you think - and they provide more of a paper trail.
    - Shop physically more than virtually - this is better for communities anyway!

H - Heed Rules

- Close down accounts they're not using - review yearly at a minimum
  - This reduces the number of ways scammers can reach your inbox
  - It also reduces the number of companies who could expose you to a data breach
  - This includes accounts that may not have financial implications - but still contain sensitive information. For example: Old medical portals, ancestry search sites, unused social media accounts, activity trackers, phone apps, physical and online stores they rarely or never visit, old work logins
- Don't use the internet on mobile devices - use a laptop or desktop with a larger screen - easier to see issues with spoofed e-mails or websites
- Avoid store credit cards & accounts:
  - Shopping as a guest is okay!
  - Often the loyalty points programs aren't worth the tracking and risk of data exposure!
  - At least limit the number of them that you use
- **Always have guard up:** basic protections work great - as long as they're followed
  - Be careful what you post! Even if you mean well, consider if you're creating exposure for someone else.
  - Check the source!
    - trusted numbers
    - spoofed e-mails
    - hang up and call the known contact back: It could be a scammer imitating your friend or family member!
    - When in doubt: stop & ask
- And if you think you may have been scammed, find out what to do next.
- If you identify a scam - a great thing to do is report it at ReportFraud.ftc.gov. Together we can help fight against this scourge!

🗨 Episode 52 Quote:

This episode’s quote is courtesy of Yuval Noah Harari, the popular author of books such as Sapiens, Homo Deus, and more:

> *One basic misconception is that people tend to equate information with truth. And information isn't true. Lies are also information. Fictions and fantasies are also information. Most information in the world is not about the truth.*